TCP/IP に係る既知の脆弱性検証ツール

取扱説明書

IPA 独立行政法人 情報処理推進機構 セキュリティセンター

2010 年 11 月

目次

◆ TCPIPCHECK（脆弱性検証ツール）編 1

1). はじめに 1
1)-1. このプログラムの目的 1
1)-2. 機能概要 1
1)-3. 動作環境 2

2). インストール 3

3). アンインストール 3

4). 基本操作 5
4)-1. 起動 5
4)-2. プロトコルの選択 5
4)-3. 脆弱性項目の選択 6
4)-3.1. 脆弱性調査報告書の表示 6
4)-3.2. IP アドレスの入力 6
4)-3.3. IP アドレスのインポート 7
4)-3.4. 監視ポート番号の入力 7
4)-3.5. ネットワーク接続名の選択 7
4)-3.6. [コピー]ボタン 7
4)-3.7. 検証を行う脆弱性項目のチェック 7
4)-3.8. パラメータのインポート 8
4)-3.9. 画面遷移 8
4)-4. パラメータの入力 8
4)-5. 検証の実行 12
4)-5.1 IP アドレスの変更 12
4)-5.2 監視ポートの変更 12
4)-5.3 詳細ログファイルの指定 12
4)-5.4 実行ボタン 13
4)-5.5 画面遷移 13
4)-6. サービス監視と脆弱性有無の判定 14
4)-7. 脆弱性項目選択画面 16
4)-7.1 詳細ログの出力 16
4)-7.2 検証結果ファイルの出力 16
4)-7.3 パラメータファイルの出力 17
4)-7.4 IP アドレスファイルの出力 18
4)-7.5 画面遷移 18
4)-8. ヘルプ 19
4)-9. 終了 19

4)-10. コマンドラインからの起動 20
4)-10.1 設定ファイル 20
4)-10.2 検証で使用するパラメータファイルと IP アドレスファイル 20
4)-10.3 検証の実行 20
4)-10.4 検証の終了 21
4)-10.5 エラー出力 21
4)-10.6 コマンドラインで起動する時の確認方法 21
4)-11. 稼動ログファイルの削除 22
4)-12. トラブルシューティング 22
4)-13. ファイル一覧 23
4)-13.1. IP アドレスファイル 23
4)-13.2. パラメータファイル 24
4)-13.3. 詳細ログファイル 27
4)-13.4. 検証結果ファイル 29
4)-13.5. 設定ファイル 30
4)-13.6. エラーログファイルの書式 32

5). 項目別検証方法 34
5)-1. TCP ISN 予測 34
5)-2. [未実装]TCP 接続の強制切断の問題 38
5)-3. SYN Flood 38
5)-4. LAND Attack 42
5)-5. Overlapping Fragment 46
5)-6. Tiny Fragment 50
5)-7. [未実装]PAWS 機能の内部タイマを不正に更新することで、TCP 通信が強制的に切断される問題 54
5)-8. [未実装]Optimistic TCP acknowledgements により、サービス不能状態に陥る問題 54
5)-9. Out Of Band 54
5)-10. [未実装]ウインドウサイズ 0 の TCP 接続過多により、サービス不能状態に陥る問題 56
5)-11. [未実装]TCP 接続状態を操作し維持させることにより、サービス不能状態に陥る問題(Naptha Attack) 56
5)-12. Ping of Death 56
5)-13. Path MTU Discovery 61
5)-14. ICMP Redirect DoS 65
5)-15. ICMP Redirect Spoofing 69
5)-16. ICMP Source Quench 73
5)-17. ICMP トンネリング 75
5)-18. ICMP blind connection reset 79
5)-19. Smurf Attack 83
5)-20. [未実装]ICMP タイムスタンプ要求/ネットマスク要求への応答による問題 88
5)-21. [未実装]IPv6 実装における Forwarding Information Base の更新に関する問題 88
5)-22. Teardrop Attack 88

5)-23. Rose Attack 93
5)-24. [未実装]IP 経路制御オプションが検査されていない問題(IP Source Routing 攻撃) 95
5)-25. IP ヘッダオプションのデータ長が 0 のパケットの問題 95
5)-26. [未実装]IP 経路制御機能(ソース・ルーティング機能)により、サービス不能状態に陥る問題 97
5)-27. IPv6 IPComp パケットの処理によりサービス不能状態に陥る問題 97
5)-28. ARP Poisoning 100
5)-29. ARP Flooding 103
5)-30. [未実装]通常ではないパケットへの応答によって OS の種類が特定できる問題(TCP/IP Stack Fingerprinting) 106
◆ TCPIPCONFIRM（脆弱性確認ツール）編 107
1). はじめに 107
5)-31. このプログラムの目的 107
5)-32. 機能概要 107
5)-33. 動作環境 107
2). インストール 108
3). アンインストール 108
4). 基本操作 109
5)-34. 起動 109
5)-35. プロトコルの選択 109
5)-36. 脆弱性項目の選択 110
4)-3.1. ネットワーク接続名の選択 110
4)-3.2. [コピー]ボタン 110
4)-3.3. 確認を行う脆弱性項目のチェック 110
4)-3.4. パラメータのインポート 111
4)-3.5. 画面遷移 111
5)-37. パラメータの入力 112
5)-38. 確認の実行 113
4)-5.1. 詳細ログの出力 113
4)-5.2. [実行]ボタン 114
4)-5.3. 画面遷移 114
5)-39. 脆弱性有無の判定 115
5)-40. 脆弱性確認画面 116
4)-7.1 詳細ログの出力 116
4)-7.2 検証結果ファイルの出力 116
4)-7.3 パラメータファイルの出力 116
4)-7.4 画面遷移 117
5)-41. ヘルプ 118
5)-42. 終了 118

5)-43. コマンドラインからの起動 119
4)-10.1 設定ファイル 119
4)-10.2 検証で使用するパラメータファイルの作成方法 119
4)-10.3 検証の実行 119
4)-10.4 検証の終了 120
4)-10.5 エラー出力 120
4)-10.6 コマンドラインで起動する時の確認方法 120
5)-44. 稼働ログファイルの削除 121
5)-45. トラブルシューティング 121
5)-46. ファイル一覧 122
4)-13.1 パラメータファイル 122
4)-13.2 詳細ログファイル 124
4)-13.3 検証結果出力ファイル 126
4)-13.4 設定ファイル 127

5). 項目別確認方法 129
5)-47. Overlapping Fragment 129
5)-48. Tiny Fragment 131
5)-49. ICMP トンネリング 133

◆ TCPIPCheck（脆弱性検証ツール）編

1). はじめに

1)-1.このプログラムの目的

TCPIPCheck は、新しく開発されたネットワーク機器に TCP/IP に係る既知の脆弱性が存在するか否かを確認するためのプログラムです。

※ すべての脆弱性を網羅してはいません。

※ 脆弱性が存在するか否かを、このプログラムだけで正確に判断はできません。

※ TCPIPCheck を実行しているコンピュータを検証対象とする事はできません。

1)-2.機能概要

攻撃シミュレーション機能

現在、インターネットプロトコル・バージョン 4（以降 IPv4）に関しては 19 件の脆弱性項目、インターネットプロトコル・バージョン 6 （以降 IPv6） に関しては 14 件の脆弱性項目の検証が可能です。これらの脆弱性の有無を確認するため、検証対象機器に対して攻撃を行います。それぞれの脆弱性の詳細は、「TCPIP に係る既知の脆弱性に関する調査報告書」の項目を参照してください。

1. TCP ISN 予測 [IPv4] [IPv6]
   参照：1) TCP の初期シーケンス番号予測の問題
2. SYN Flood [IPv4] [IPv6]
   参照：3) SYN パケットにサーバ資源が占有される問題（SYN Flood Attack）
3. LAND Attack [IPv4] [IPv6]
   参照：4) 特別な SYN パケットによりカーネルがハングアップする問題（LAND Attack）
4. Overlapping Fragment [IPv4] [IPv6]
   参照：5) データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題（Overlapping Fragment Attack）
5. Tiny Fragment [IPv4] [IPv6]
   参照：6) 十分に小さい分割パケットがフィルタリングをすり抜ける問題 （Tiny Fragment Attack,Tiny Overlapping Fragment Attack）
6. Out Of Band [IPv4]
   参照：9) Out Of Band(OOB)パケットにより、サービス不能状態に陥る問題
7. Ping of Death [IPv4] [IPv6]
   参照：12)パケット再構築時にバッファが溢れる問題（Ping of Death）
8. Path MTU Discovery [IPv4] [IPv6]
   参照：13) ICMP Path MTU Discovery 機能を利用した通信遅延の問題
9. ICMP Redirect DoS [IPv4] [IPv6]

参照：14) ICMP リダイレクトによるサービス応答遅延の問題

10. ICMP Redirect Spoofing [IPv4] [IPv6]
    参照：15) ICMP リダイレクトによる送信元詐称の問題
11. ICMP Source Quench [IPv4]
    参照：16) ICMP 始点制御メッセージによる通信遅延の問題
12. ICMP トンネリング[IPv4] [IPv6]
    参照：17) ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題(ICMP トンネリング)
13. ICMP blind connection reset [IPv4] [IPv6]
    参照：18) ICMP エラーにより TCP 接続が切断される問題
14. Smurf Attack [IPv4] [IPv6]
    参照：19) ICMP Echo リクエストによる帯域枯渇の問題（Ping Flooding, Smurf Attack, Fraggle Attack）
15. Teardrop Attack [IPv4] [IPv6]
    参照：22) フラグメントパケットの再構築時にシステムがクラッシュする問題（Teardrop Attack）
16. Rose Attack [IPv4]
    参照：23) パケット再構築によりメモリ資源が枯渇される問題（Rose Attack）
17. IP ヘッダオプションのデータ長が 0 のパケットの問題[IPv4]
    参照：25) IP ヘッダオプションのデータ長が 0 のパケットの問題
18. IPv6 IPComp パケット [IPv6]
    参照：27) IPv6 IPComp パケットの処理によりサービス不能状態に陥る問題
19. ARP Poisoning [IPv4]
    参照：28) ARP テーブルが汚染される問題
20. ARP Flooding [IPv4]
    参照：29) ARP テーブルが不正なエントリで埋め尽くされる問題

<u>サービス監視機能</u>

検証対象の機器に対して、任意の TCP ポートが接続可能かどうかを、検証中と検証終了後に定期的に監視し、脆弱性に対する効果の有無を調査することができます。接続不能な状態が指定した回数発生すると、効果が有ったと判定をします。ただし、脆弱性に対する効果の有無は、この機能だけでは判断することはできません。本取扱説明書には脆弱性毎に脆弱性の有無を確認する方法が記載されているので、その際に判断する 1 つの材料として活用してください。

1)-3.動作環境

TCPIPCheck は、以下のコンピュータ上で動作します。

Microsoft Windows XP Professional SP3 が動作する IBM AT 互換機
CD-ROM ドライブ、NIC を有する事

また、以下の環境を推奨します。

CPU	: Intel Pentium 4　2GHz 以上
ディスプレイ	: 画面解像度 1024 x 768 ピクセル以上
メモリ	: 1GBytes 以上
ハードディスク	: 1GBytes 以上の空き容量
NIC	: Ethernet(100M 以上）のインターフェイスを有する事

2). インストール

以下の手順で、インストールを行ってください。

※ 前バージョンがインストールされている時には、前バージョンをアンインストールしてから、以下の 2.の手順からインストールを行なってください。

※ 後述の TCPIPConfirm （脆弱性確認ツール） がインストールされている時、TCPIPCheck をインストールすることはできません。TCPIPConfirm をアンインストールしてから、以下の 2.の手順からインストールを行ってください。TCPIPConfirm のアンインストール方法は、TCPIPConfirm（脆弱性確認ツール）編 3).アンインストール）を参照してください。

※ インストールを行う時は、Administrators 権限を持つアカウントでインストールを行ってください。

1. 以下のサイトから、WinPcap (Windows Packet Capture Library) のインストーラをダウンロードし、インストールを行ってください。
   http://www.winpcap.org/install/default.htm
   WinPcap4.0.2 (2008 年 8 月 26 日最新) “WinPcap auto-installer (Driver +DLLs)”あるいは WinPcap4.1.1 (2010 年 7 月 2 日最新) “WinPcap auto-installer (Driver +DLLs)”
2. TCPIPCheck インストール CD を CD ドライブにセットします。
3. スタートメニューから、[ファイル名を指定して実行]を選択し、”<CD ドライブ>:¥TCPIPCheck¥ Setup.Exe”をタイプし、[OK]ボタンをクリックします。
4. インストーラが起動し、TCPIPCheck のインストールが開始されます。
5. この後の手順は、インストーラの指示に従って、インストールを行ってください。

3). アンインストール

以下の手順で、アンインストールを行ってください。

1. [スタートメニュー]-[コントロールパネル]-[プログラムの追加と削除]を選択してください。
2. [プログラムの追加と削除]ダイアログから、TCPIPCheck の項目を選択し、[削除]ボタンを

クリックしてください。TCPIPCheck のアンインストールが開始されます。

3. 後は、インストーラの指示に従って、アンインストールを行ってください。
4. 同じく、[プログラムの追加と削除]ダイアログから、WinPcap を選択し、[変更と削除]ボタンをクリックしてください。
5. [WinPcap Uninstall]ダイアログの[Uninstall]ボタンをクリックしてください。
6. この後の手順は、インストーラの指示に従って、アンインストールを行ってください。

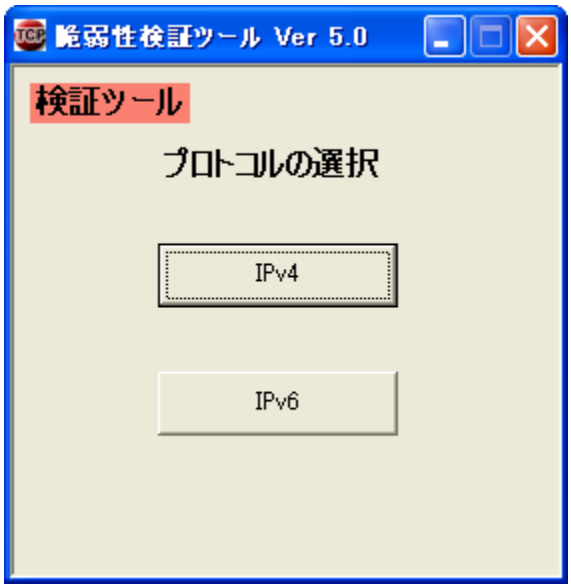
※ 4～6 は任意です。

4). 基本操作

4)-1.起動

スタートメニューから、[プログラム]-[IPA]-[TCPIPCheck]を選択してください。プログラムが起動します。起動は Administrators 権限を持つユーザで行ってください。

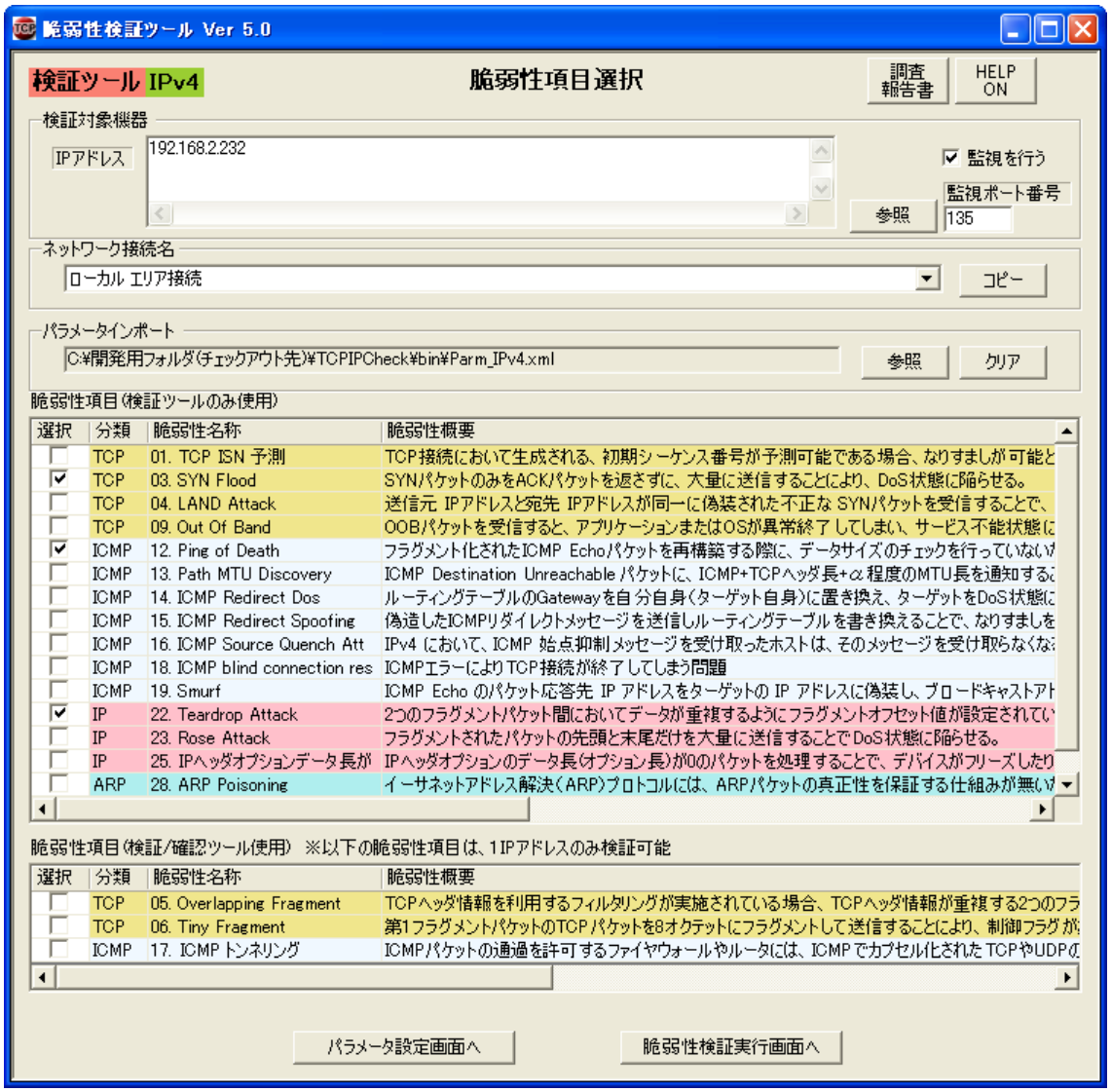
4)-2.プロトコルの選択



プロトコル選択画面では、以下の操作を行います。

1. 検証を行うプロトコルを選択します。
   "ネットワーク接続情報を取得できませんでした"と表示される時、プロトコルが正しくインストールされているか確認してください。

4)-3.脆弱性項目の選択



脆弱性項目選択画面では、以下の操作を行います。

4)-3.1. 脆弱性調査報告書の表示

[調査報告書]ボタンをクリックした時、TCPIP に係る既知の脆弱性に関する調査報告書(pdf ファイル)が開かれます。使用している PC に pdf ファイルを閲覧することができるソフトが存在していなかった時は、”pdf を開くことができるアプリケーションがありません”と表示されます。 TCPIP に係る既知の脆弱性に関する調査報告書の内容を確認したい時は、pdf を開くことができるアプリケーションをインストールしてください。

4)-3.2. IP アドレスの入力

検証対象機器の IP アドレスを入力します。1 行に 1IP しか入力できず、カンマ区切りでの

指定は行えません。一行に複数の IP アドレスを入力したい場合は範囲指定で行い、第 4 オクテット(IPv6 の時は、第 8 オクテット)に対してハイフンを使用することで行えます。最大 255 行まで検証が行われます。

4)-3.3. IP アドレスのインポート

本ツールでは、IP アドレスのインポートを行うことができます。

この機能により、同一対象に対して複数回の検証を行う時でも、毎回手動で同じ IP アドレスを入力することなく簡単に対象機器への設定が行えます。

1. インポートを行う手順

[参照]ボタンをクリックした時、[ファイルを開く]ダイアログが表示されるので、IP アドレスが記載されているファイルを選択します。ファイル内に記載されている空白行とコメント行(4)-13.1 参照)を除く全てのデータが、IP アドレス入力欄に入力されます。

2. インポートに使用するファイル

ファイルフォーマットに関しては、[4)-13.1]を参照してください。

4)-3.4. 監視ポート番号の入力

サービス監視のための監視ポート番号を入力します。このポート番号は、検証対象機器で OPEN 状態である必要があります。OPEN 状態でないポート番号を入力した時は、[次へ]ボタンをクリックした際にエラーとなります。サービス監視を行わない時には、[監視を行う]チェックボックスを、チェックをしない状態にしてください。

4)-3.5. ネットワーク接続名の選択

検証を行う際に使用するネットワーク接続名を選択します。選択したネットワーク接続名を用いて、脆弱性パケットの送信と受信が行われます。

1. ネットワーク接続名の選択方法

TCPIPCheck をインストールしたコンピュータで、複数の有効なネットワーク接続名が存在する時には、[ネットワーク接続名]コンボボックスに複数のネットワーク接続名がセットされています。検証に使用するネットワーク接続名を選択してください。

4)-3.6. [コピー]ボタン

クリップボードに選択しているネットワーク接続名をコピーします。コマンドライン起動を行う際に必要な設定ファイル[4)-13.5 参照]の作成を補助する機能です。利用方法は[4)-13.5]の、ConnectionName の欄を確認してください。

4)-3.7. 検証を行う脆弱性項目のチェック

検証を行う脆弱性項目の左の[選択]チェックボックスをチェックします。複数の項目をチェ

ックすることが可能です。複数の項目をチェックした時、選択された脆弱性項目のパラメータを入力後、連続して検証を行います。この時、サービス監視機能で脆弱性有りと判断された時点で、検証は終了し、以降の脆弱性項目の検証を行いません。

4)-3.8. パラメータのインポート

本ツールではパラメータファイルのインポートを行うことができます。パラメータのインポートを行うことにより、検証対象機を変更しても再び同じパラメータファイルをインポートすることにより、同じパラメータで検証を行うことができます。

1. パラメータのインポート方法
   パラメータインポートの[参照]ボタンをクリックした時、[ファイルを開く]ダイアログが表示されるので、パラメータが入力されている xml ファイルを指定します。xml ファイルからパラメータがインポートされます。この時、パラメータのインポートが行われた脆弱性は[選択]チェックボックスにチェックがつきます。
2. インポートに使用するファイル
   ファイルフォーマットに関しては、[4)-13.2]を参照してください。
3. [クリア]ボタン
   パラメータのインポートを行った時、[クリア]ボタンが選択可能になります。[クリア]ボタンをクリックした時、全ての脆弱性の[選択]チェックボックスからチェックが外れ、入力されていたパラメータが全て空白になります。また、[脆弱性実行画面へ]ボタンが選択不可になります。

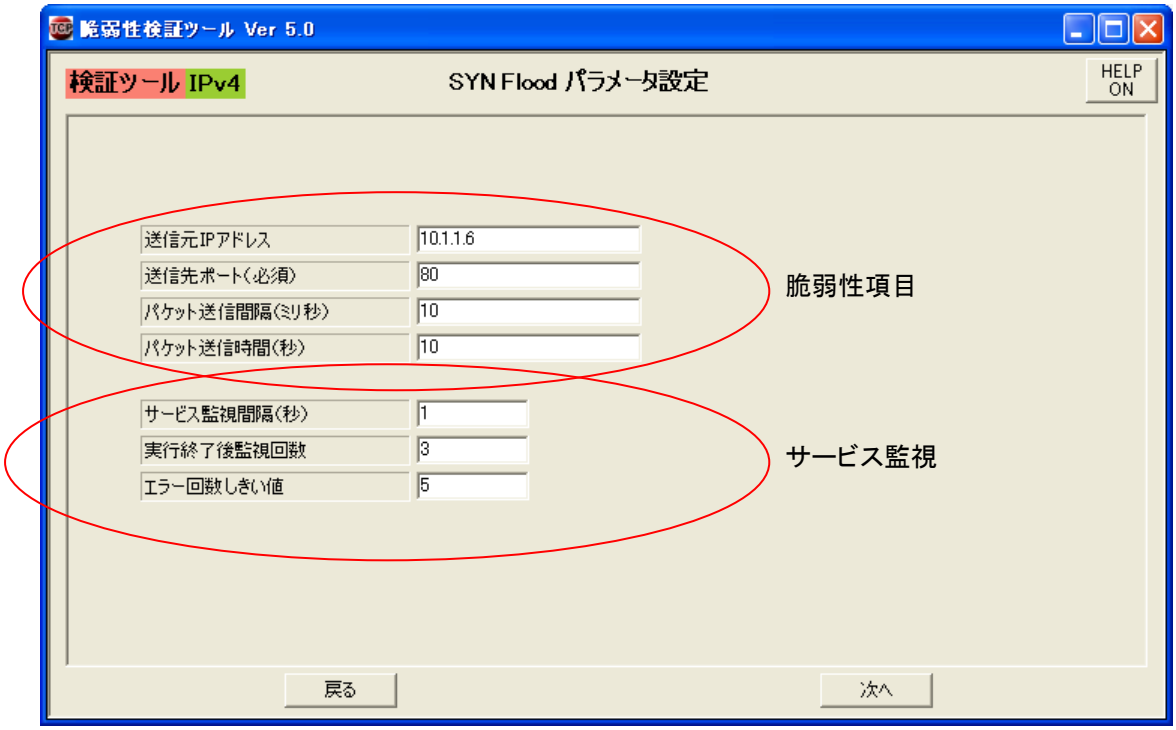
4)-3.9. 画面遷移

1. [パラメータ設定画面へ]ボタン
   [パラメータ設定画面へ]ボタンをクリックした時、パラメータ設定画面へと遷移します。
2. [脆弱性実行画面へ]ボタン
   パラメータのインポートを行った時、[脆弱性実行画面へ]ボタンが選択可能になります。[脆弱性実行画面へ]をクリックした時、選択した全ての脆弱性に対してパラメータのチェックが行われ、脆弱性実行画面に遷移します。

4)-4.パラメータの入力

選択された脆弱性項目のパラメータ入力画面が順次表示されます。脆弱性項目によって入力が必要な項目は変わります。

下の 3 つの項目は、サービス監視のためのパラメータです。脆弱性項目選択画面で、[監視を行う] チェックボックスをチェックしない状態にした時は、これらのパラメータは表示されません。



パラメータ設定画面では、以下の操作を行います。

1. 脆弱性項目のパラメータを入力します。
2. サービス監視パラメータを入力します。
3. パラメータ入力が完了しましたら、[次へ]ボタンをクリックしてください。
   次の脆弱性項目のパラメータ設定画面、または、脆弱性検証実行画面に移ります。
4. 前の画面に戻りたい時には、[戻る]ボタンをクリックしてください。
   前の脆弱性項目のパラメータ設定画面、または、脆弱性項目選択画面に戻ります。

※ パラメータの詳細は、0.項目別検証方法を参照してください。

脆弱性監視項目の設定について

脆弱性監視項目に関する以下のパラメータが設定可能です。入力範囲は以下の通りです。

パラメータの種類	入力範囲
IP アドレス	IPv4 の場合、プライベートアドレス(10.0.0.0/8,172.16.0.0/12,192.168.0.0/16)のみ入力できます。 IP v 6 の場合、リンクローカルアドレス(FE80::/64)又はユニークローカルユニキャストアドレス(FC00::/7)のみ入力できます。 （ネットワークの設定・接続が正しく行われていない時、IP アドレスの入力エラーとなる時があります。） ※複数の IP アドレスの指定については、4)-3. 脆弱性項目の選択の 1 を参照してください。
ポート番号	1～65,535 を入力できます。
パケット送信回数	1～1,000,000 を入力できます。
パケット送信時間（秒）	1～1,000,000 を入力できます。
パケット送信間隔（ミリ秒）	0～65,535 を入力できます。ミリ秒単位ですが、OS の制限により、15 ミリ秒以下は設定できません。0 ミリ秒は間隔を置かずに送信します。
上記以外の数値	パラメータ毎に範囲が異なります。

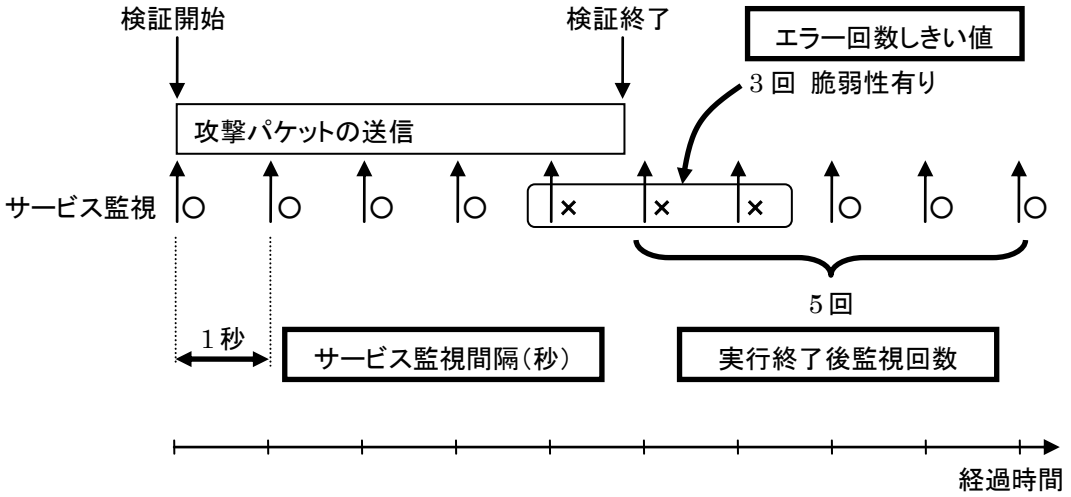
サービス監視の設定について

サービス監視機能に関する以下のパラメータが設定可能です。

パラメータの種類	説明
サービス監視間隔（秒）	サービス監視を行う間隔を秒数で指定します。 攻撃パケットの送信開始時点から、送信終了後、次のパラメータの実行終了後監視回数が終了するまで、指定した秒間隔でサービス監視を行います。 1 秒程度の値を推奨いたします。この値を大きくすると、判定が甘くなる可能性があります。
実行終了後監視回数	攻撃パケットの送信が終了後、サービス監視を行う回数を指定します。 5 回程度の値を推奨いたします。 攻撃パケットの送信終了後に、攻撃の影響がでると予想される時には、この値を大きくしてください。
エラー回数しきい値	サービス監視における脆弱性有無の判定に使用するしきい値です。 しきい値で指定した回数分連続して接続できなかった時に、脆弱性有りと判断します。 3 回程度の値を推奨いたします。

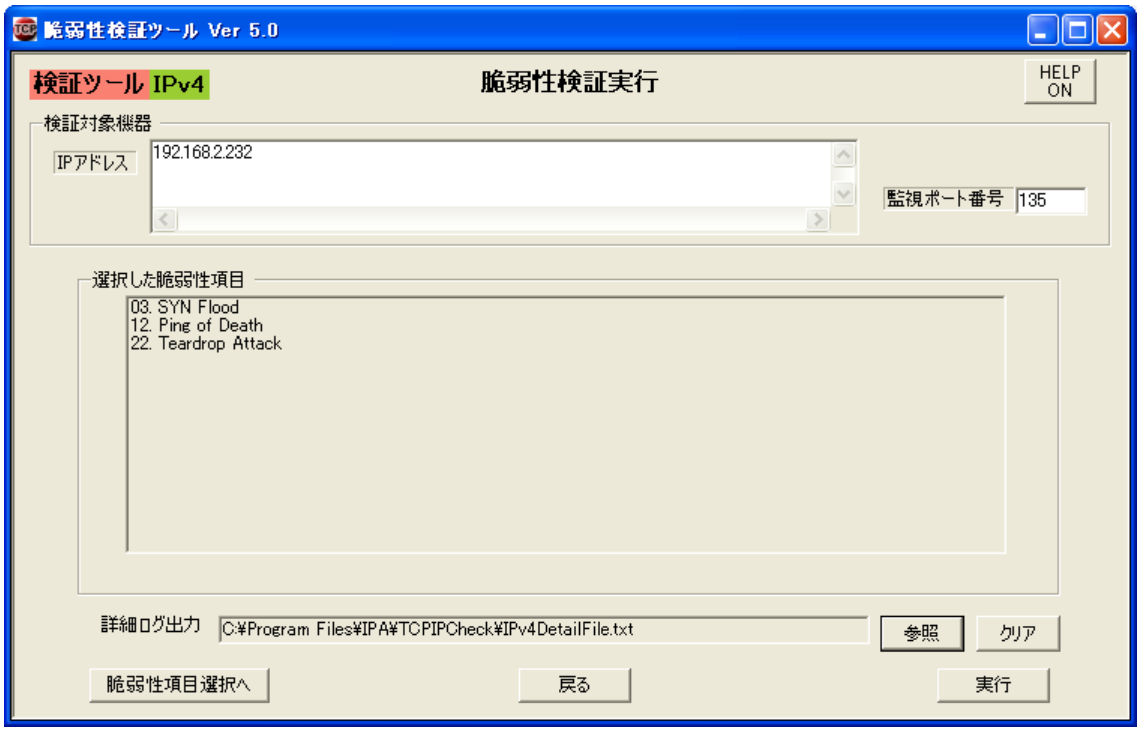
	しきい値で指定した回数に達しないが、1 回でも接続できなかった時には、脆弱性有りの疑いと判断します。

以下は、サービス監視の動作とパラメータ値の関係を図で示したものです。



4)-5.検証の実行

脆弱性検証実行画面が表示されます。



脆弱性検証実行画面では、以下の操作を行います。

4)-5.1 IP アドレスの変更

検証対象機器の IP アドレスを変更することができます。

4)-5.2 監視ポートの変更

監視ポート番号を変更することができます。

脆弱性項目選択画面で[監視を行う]チェックボックスをチェックしない状態にした時、この項目は入力できません。

4)-5.3 詳細ログファイルの指定

本ツールでは、詳細ログの出力を行うことができます。詳細ログを出力することにより、各検証結果の比較を行うことができ、エラー発生時にその情報が出力されるようになります。指定を行わなかった時、詳細ログの出力は行われません。

1. 詳細ログの指定方法

[参照]ボタンをクリックした時、[名前を付けて保存]ダイアログが開かれるので詳細ログの出力先を指定します。その場合、検証終了後に指定したファイルにテキストファイルでツールの詳細ログが出力されます。また、詳細ログファイルの指定は出力先を直接指定する

ことはできません。

2. 詳細ログファイルの書式
   ファイルフォーマットに関しては、[4)-13.3]を参照してください。
3. クリアボタン
   詳細ログを指定した時、[クリア]ボタンが選択できるようになります。[クリア]ボタンをクリックした時、詳細ログの指定がキャンセルされ、詳細ログは出力されません。

4)-5.4 実行ボタン

[実行]ボタンをクリックすると、検証が開始され、脆弱性検証確認画面に移ります。このとき詳細ログファイルの指定に既存のファイルを指定した時､ファイルに追記する旨を確認するメッセージボックスが表示されます。追記しても問題が無い時は[はい]を選択してください。[いいえ]を選択した時、脆弱性実行画面へ遷移します。

4)-5.5 画面遷移

1. [戻る]ボタンをクリックすると、前の脆弱性項目のパラメータ設定画面に戻ります。

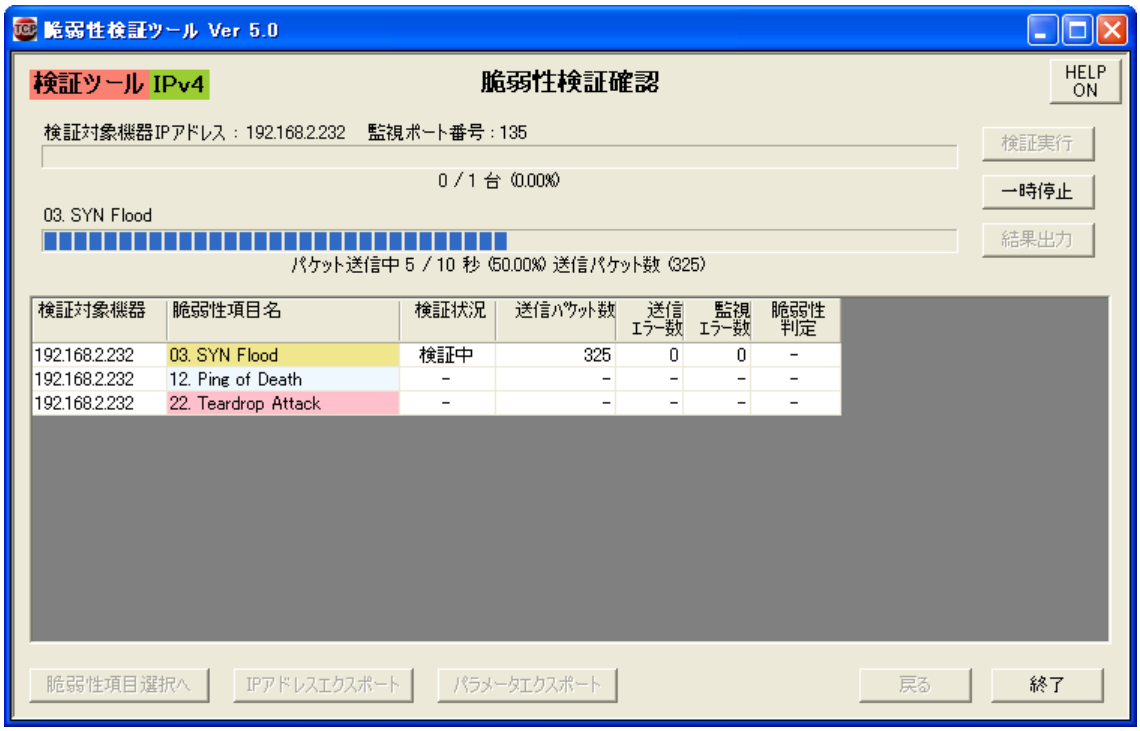
2. [脆弱性項目選択へ]ボタンをクリックすると、脆弱性項目選択画面に戻ります。

4)-6.サービス監視と脆弱性有無の判定

検証実行中、検証終了後は、脆弱性検証確認画面が表示されます。

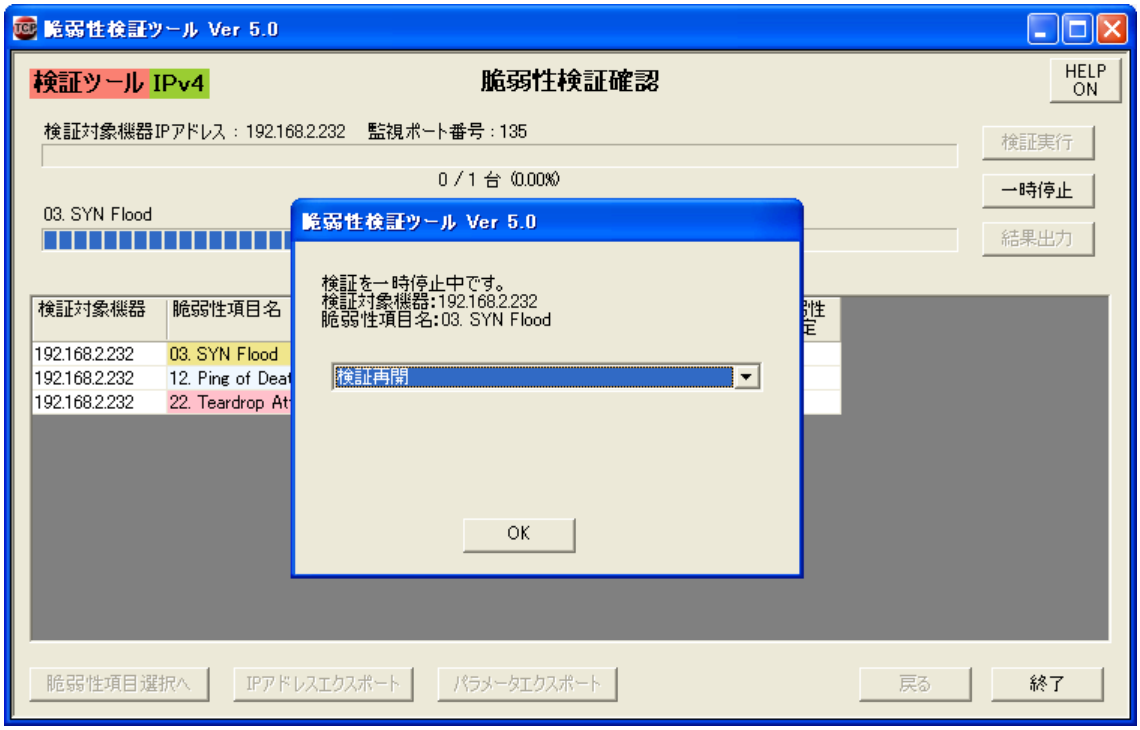
以下は、検証実行中の画面の例です。

脆弱性項目毎の検証状況、脆弱性判定を表示します。


脆弱性検証ツール Ver 5.0
検証ツール IPv4
脆弱性検証確認
HELP ON
検証対象機器IPアドレス：192.168.2.232　監視ポート番号：135
検証実行
0 / 1 台 (0.00%)
一時停止
03. SYN Flood
結果出力
パケット送信中 5 / 10 秒 (50.00%) 送信パケット数 (325)
検証対象機器 | 脆弱性項目名 | 検証状況 | 送信パケット数 | 送信エラー数 | 監視エラー数 | 脆弱性判定
192.168.2.232 | 03. SYN Flood | 検証中 | 325 | 0 | 0 | -
192.168.2.232 | 12. Ping of Death | - | - | - | - | -
192.168.2.232 | 22. Teardrop Attack | - | - | - | - | -
脆弱性項目選択へ
IPアドレスエクスポート
パラメータエクスポート
戻る
終了

[一時停止]ボタンをクリックすると、検証を一時停止します。

検証の再開、再実行、中止を選択できます。



検証状況には、以下の表示があります。

表示内容	説明
ー	まだ実行されていません。
検証中	検証を行っています。
監視中	サービスの監視を行っています。
検証エラー	攻撃パケットの送信処理において、エラーが発生しました。 ネットワークの接続を確認してください。また、送信間隔とパケット送信回数を調整して、再度検証を行ってください。
中止	[一時停止]ボタンをクリック後、検証が中止されました。
スキップ	脆弱性判定結果が有り、又は、検証エラーの時、残りの脆弱性項目の検証をスキップし、次の対象機器の検証を開始します。
完了	検証と監視が終了しました。

脆弱性判定には、以下の表示があります。

表示内容	説明
ー	まだ判定されていません。あるいは、サービス監視を行いませんでした。 あるいは、検証がエラーとなりました。
無し	サービス監視で異常はありませんでした。
有り	サービス監視で異常の回数がしきい値に達しました。
有りの疑い	サービス監視で異常がありましたが、回数がしきい値に達しませんでした。

TCPIPCheck の脆弱性判定機能は、単純なサービスポートの監視結果を見ているに過ぎません。実際の脆弱性の有無は、検証対象機器の状態を、検証者が確認する必要があります。

実際の脆弱性有無の確認方法については、0.項目別検証方法を参照してください。

4)-7.脆弱性項目選択画面

4)-7.1 詳細ログの出力

本ツールでは詳細ログが指定されている場合、検証途中で出力されるログと、検証終了時にユーザが指定したファイルに出力される詳細ログの、二種類を出力します。

1. 検証途中で出力されるログ
   脆弱性の検証中、各実行プログラムは以下のファイルに詳細ログを出力していきます。

   <インストールディレクトリ>¥logs¥[脆弱性のプログラム番号].log

   これらのファイルには脆弱性毎の検証状況が記載されています。ツールが正常終了した時、出力されたファイルはフォルダ内から削除されます。
   検証ツールが異常終了した時、これらのファイルは削除されないため、どの処理を行っている時にツールが終了したのか、内容を閲覧することで確認することが可能です。
2. 検証終了時に出力される詳細ログ
   詳細ログの指定を行っていた時、ユーザが指定したファイルに詳細ログの追記が行われます。

4)-7.2 検証結果ファイルの出力

本ツールでは、検証結果ファイルを出力することができます。検証結果の出力を行うことにより、検証結果の保存と各検証結果の比較等も行えます。

1. 検証結果の出力方法
   [結果出力]ボタンをクリックした時、[名前を付けて保存]ダイアログが表示され検証結果ファイルの出力先を指定できます。ファイルを指定した時、新規ファイルである時は作成がそのまま行われます。既存のファイルを指定している時は追記を行ってもよいか確認するメッセージボックスが表示されます。[はい]を選択した時、指定したファイルに検証結果が出力されます。[いいえ]を選択した時、検証結果は出力されません。
2. 検証結果ファイルの形式
   ファイルフォーマットに関しては、[4)-13.4]を参照してください。

4)-7.3 パラメータファイルの出力

本ツールでは、検証に使用したパラメータを xml ファイルでエクスポートすることができます。エクスポートしたファイルは、パラメータのインポートで使用することができます。

1　パラメータファイルの作成

[パラメータエクスポート]ボタンをクリックした時、[名前を付けて保存]ダイアログが表示されるのでファイルを指定すると、検証で設定したパラメータをファイルにエクスポートすることができます。新規のファイルを指定した時はそのまま出力が行われますが、既存のファイルを指定した時は上書きを行うか確認する旨を記載したメッセージボックスが表示され、[はい]を選択すると指定したファイルに上書きされます。[いいえ]を選択すると、処理は終了します。

2　パラメータファイルの形式

出力されるファイルの形式は、パラメータインポートでインポートしたファイルと同じ内容です。詳しくは、[4)-13.2]を参照してください。

4)-7.4 IP アドレスファイルの出力

本ツールでは、検証対象とした IP アドレスの一覧を txt ファイルでエクスポートすることができます。エクスポートしたファイルは、IP アドレスのインポートで指定することにより、同じ対象に対して検証が実行できます。

1. IP アドレスファイルの作成

   [IP アドレスエクスポート]ボタンをクリックした時、[名前を付けて保存]ダイアログが表示されるのでファイルを指定すると、今回の検証で使用したパラメータが登録されているパラメータファイルのエクスポートが行えます。新規のファイルを指定した時はそのまま出力が行われますが、既存のファイルを指定した時は上書きを行うか確認する旨を記載したメッセージボックスが表示され、[はい]を選択した時、指定したファイルに上書きされます。[いいえ]を選択した時、処理は終了します。

2. IP アドレスファイルの書式

   出力されるファイルの内容と形式は、IP アドレスインポートでインポートしたファイルと同じ内容です。詳しくは、[4)-13.1]を参照してください。

4)-7.5 画面遷移

1. [戻る]ボタン

   [戻る]ボタンをクリックした時、脆弱性実行画面へと遷移します。

2. [脆弱性項目選択へ]ボタン

   [脆弱性項目選択へ]ボタンをクリックした時、脆弱性選択画面へと遷移します。

4)-8.ヘルプ

各画面の[HELP ON]ボタンをクリックすると、ヘルプ画面を表示します。各画面の説明と、脆弱性解説の 2 種類のヘルプを参照できます。[連動する]チェックボックスをチェックすると、画面の遷移に応じてヘルプの表示内容も切り替わります。

4)-9.終了

脆弱性検証確認画面の[終了]ボタン、あるいは、各画面のタイトルバーの右端にある終了ボタンをクリックすると、プログラムが終了します。

4)-10.コマンドラインからの起動

本ツールでは、GUI 操作では対応することが難しい、ツールの自動化(バッチ処理)に対応するため、コマンドラインで起動することもできます。コマンドラインで起動するためには、あらかじめ以下のファイルを用意しておく必要があります。

・設定ファイル
・IP アドレスファイル
・パラメータファイル

4)-10.1 設定ファイル

コマンドラインで起動する際にパラメータとして指定するファイルです。コマンドライン起動時の処理は、設定ファイルに指定された内容で実行されます。書式は、[4)-13.5]を参照してください。

4)-10.2 検証で使用するパラメータファイルと IP アドレスファイル

IP アドレスファイルは、[4)-13.1]の形式のものを使用し、パラメータファイルは[4)-13.2]の形式のものを使用してください。指定したファイルに記載されている内容に則って検証が行われます。

4)-10.3 検証の実行

1. コマンドプロンプト上で TCPIPCheck.exe を起動させ、パラメータとして設定ファイルを指定します。設定ファイルの内容の通り、検証が実行されます。以下に実行例を記載します。

4)-10.4 検証の終了

正常に検証が終了した場合、設定ファイルで指定した場所に検証結果ファイルが出力されます。詳細ログファイルは設定ファイルで指定されている時のみ出力されます。

4)-10.5 エラー出力

コマンドラインでの起動中、正常に検証が行えなかった時や処理が異常終了した時、エラーログファイルとイベントログにエラー情報が記載されます。ファイルの書式は、[4)-13.6]を参照してください。

1. イベントログへの出力

コマンドラインの起動中、エラーが起きた時はイベントログへの出力が行われます。
イベントログへの出力は以下の時に行われます。

・ツールの起動時
・ツールの終了時
・エラー発生時

イベントログの出力を確認したい時は[コントロールパネル]-[管理ツール]-[イベントビューア]-[アプリケーション]を確認してください。
このツールが出力したイベントログを参照したい時は、イベントソースで[脆弱性検証ツール Ver 5.0]で検索を行ってください。

4)-10.6 コマンドラインで起動する時の確認方法

コマンドライン起動時、以下のタイミングで動作を確認する方法を記載します。

1. 起動の確認

イベントログに開始が書き込まれているか確認を行ってください。

2. 検証状況の確認

詳細ログの出力行っている時、<インストールディレクトリ>¥log フォルダに、モジュールが出力したログが作成されるので、その内容をご確認ください。なお、これらのログはツールが正常終了した場合、削除されます。

3. 検証結果の確認

設定ファイルで指定した検証結果ファイルと詳細ログファイルに検証結果と詳細ログが出力されるので、内容をご確認ください。

4)-11.稼動ログファイルの削除

下記のディレクトリに稼動状況を記録した月別のログファイルを作成しています。これらのファイルは自動的には削除されませんので内容を確認し、不要なファイルは削除してください。内容の確認は[スタートメニュー]-[すべてのプログラム]-[アクセサリ]-[メモ帳]で行えます。（その他のテキストエディタでも内容の確認は可能です。）

- IPv4 の稼動ログファイルディレクトリ
  <インストールディレクトリ>¥log_IPv4
- IPv6 の稼動ログファイルディレクトリ
  <インストールディレクトリ>¥log_IPv6

4)-12.トラブルシューティング

以下のようなエラーメッセージが頻繁に表示される時は、TCPIPCheck を再インストールする事を推奨します。3).アンインストールを実行後、2).インストールを実行してください。エラーメッセージは、コマンドライン起動時はイベントログとエラーログ、画面で起動している時はメッセージボックスで表示されます。また、TCPIPCheck を実行しようとした時にインストーラが作動してしまう時も、検証実行に必要なファイルが削除されている可能性がありますので、同様に再インストールする事をお勧めします。

主な、深刻なエラーメッセージは以下の通りです。

エラーメッセージ	エラー内容
ネットワーク接続名を取得出来ませんでした。	NIC が正しく接続されていないか、ネットワーク接続が無効となっている時に出力されます。 ネットワークの設定を確認してください。
設定ファイルを読み込めませんでした。	設定ファイル（config_IPv4.xml または config_IPv6.xml）に不具合がある時に出力されます。 再インストールする事をお勧めします。
設定ファイルに脆弱性情報が正しく定義されていません。	
設定ファイルの ID が重複しています。 id=nnnn	
脆弱性検証モジュール（0xx.exe）の実行に失敗しました。 エラーコード = 1、又は -1	検証モジュールが他のプロセスから強制終了されてしまった時に出力されます。 もう一度、検証を実行してみてください。
脆弱性検証モジュール（0xx.exe）の実行に失敗しました。	検証開始時に、検証対象機器と接続出来ない時に出力されます。

エラーコード = -100 ～ -199	
脆弱性検証モジュール（0xx.exe）の実行に失敗しました。	検証モジュールexeファイルが存在しない時に出力されます。 再インストールする事をお勧めします。
検証対象機器に接続出来ませんでした。	WinPcapが使用出来ない時等に出力されます。 再インストールする事をお勧めします。
ディスクの容量が一杯になりました。	ファイルを出力しようとした先の空き容量が1M以下となっている時に出力されます。出力先のドライブに空き容量を作成してからファイルを出力し直してください。
コマンドライン起動設定ファイルが読み込めませんでした	コマンドライン起動時のみ出力されます。 指定した設定ファイルが読み込めなかった時に表示されます。パラメータと、指定した設定ファイルの内容を確認してください。

4)-13.ファイル一覧

本ツールで用いられるファイルについて説明します。

4)-13.1. IPアドレスファイル

検証対象機器のIPアドレスを指定するファイルです。
作成は、脆弱性確認画面の[IPアドレスエクスポート]ボタンで作成するか、以下のフォルダ内にあるサンプルファイルを編集することで作成してください。

IPv4のIPアドレスファイル
<インストールディレクトリ>¥サンプル¥IPv4¥ IPv4IPFile.txt

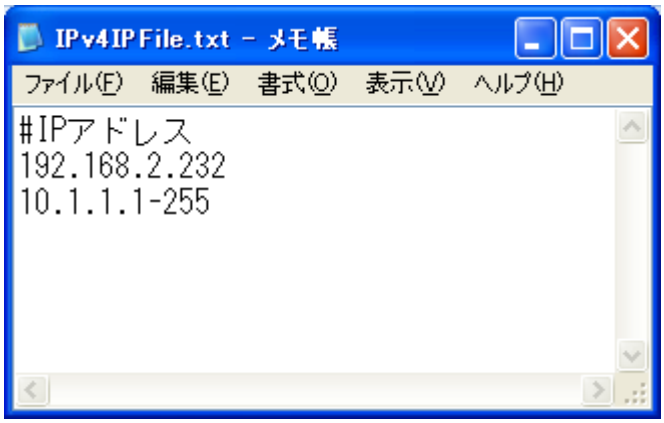
IPv6のIPアドレスファイル
<インストールディレクトリ>¥サンプル¥IPv6¥ IPv6IPFile.txt

内容は以下の通りです。

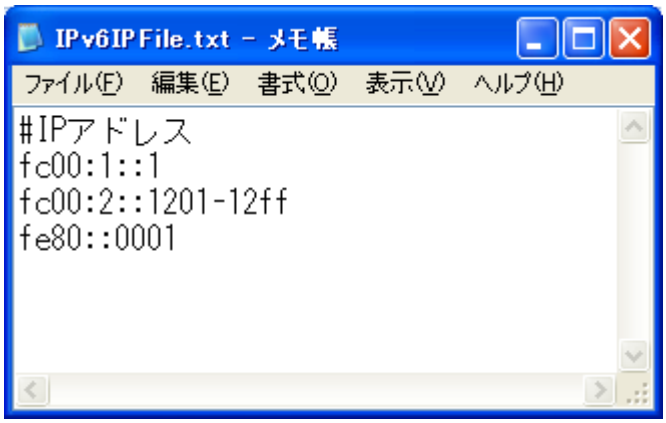
・テキスト形式で作成する
・1つのIPアドレス指定ごとに改行する
・先頭が#の文は、コメント行として扱われる。コメント行はインポートされない
・空白行はインポートされない
・最大255行(コメント行および空白行は含まない)までにしてください。256行以上入力されていた時、検証が実行できません

以下に IP アドレスファイルのサンプルを記載します。

IPv4



IPv6



4)-13.2. パラメータファイル

脆弱性項目の名称や各種パラメータ設定を記載するファイルです。

検証に使用するパラメータファイルは、パラメータのエクスポートで作成するか、以下のフォルダ内に存在するサンプルファイルを編集することで作成してください。パラメータファイルの作成は、パラメータエクスポートで行うことを推奨いたします。

その場合、以下の内容で編集を行ってください。書式は xml 規格に準じます。

XML タグ	説明
config id	脆弱性の config id を入力します。
name	脆弱性項目名を入力します。
monitoring	ツールのサービス監視関連の情報を定義します。
interval	サービス監視間隔(秒)を指定します。
after-count	検証モジュール実行終了後にサービス監視を行う回数を指定します。
error-count	しきい値(連続接続エラー回数)を指定します。
parameter identifier	検証モジュールの個別パラメータごとに定義します。 属性 identifier にはパラメータ識別子を指定します。
param-name	パラメータ入力画面のラベルとして指定します。
param-type	IP アドレスの入力補正を行う項目の時に指定します。
value	入力値を指定します。

以下にパラメータファイルのサンプルを記載します。

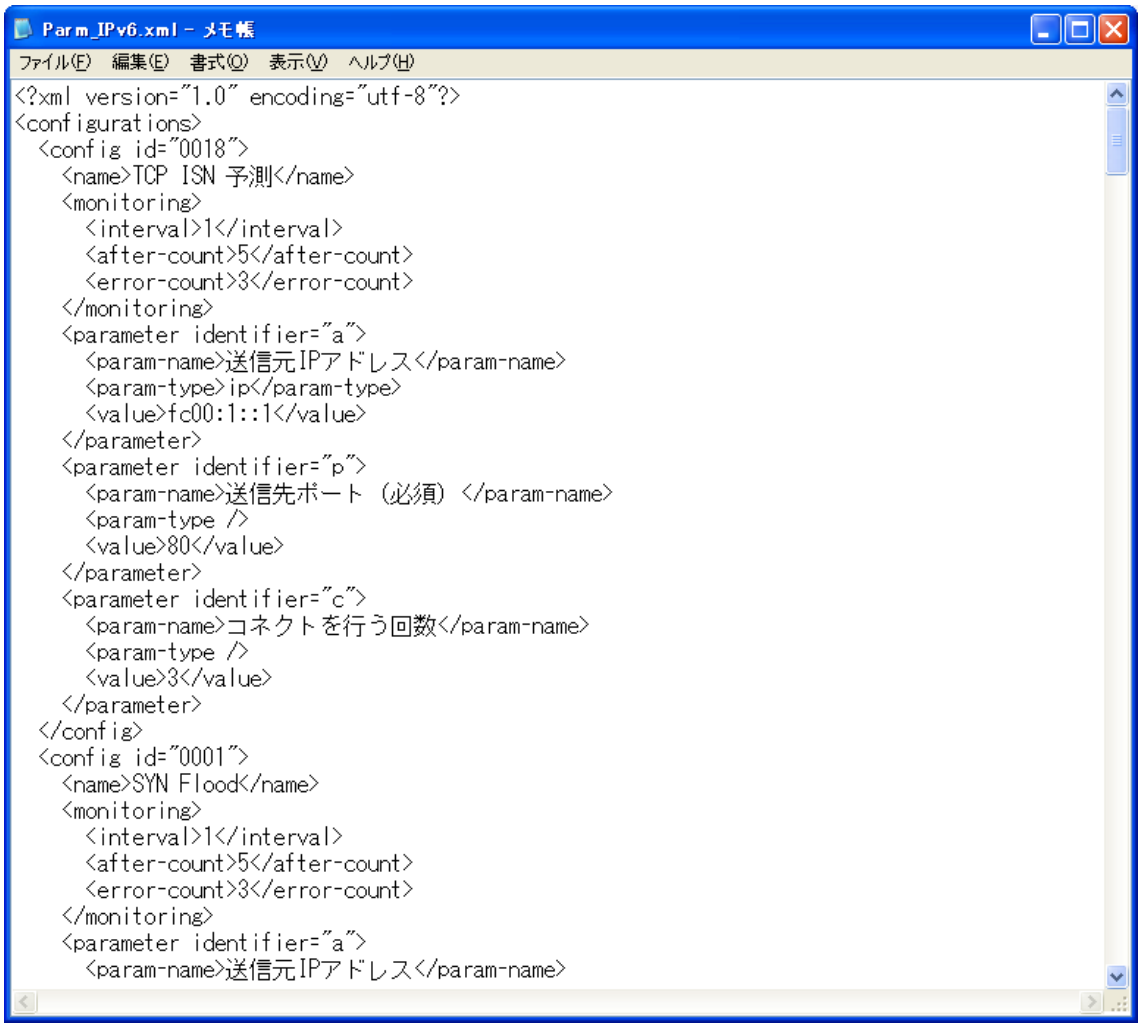
IPv4

Parm_IPv4.xml - メモ帳

ファイル(F)　編集(E)　書式(O)　表示(V)　ヘルプ(H)

```
<?xml version="1.0" encoding="utf-8"?>
<configurations>
  <config id="0001">
    <name>SYN Flood</name>
    <monitoring>
      <interval>1</interval>
      <after-count>3</after-count>
      <error-count>5</error-count>
    </monitoring>
    <parameter identifier="a">
      <param-name>送信元IPアドレス</param-name>
      <param-type>ip</param-type>
      <value>10.1.1.6</value>
    </parameter>
    <parameter identifier="p">
      <param-name>送信先ポート（必須）</param-name>
      <param-type />
      <value>80</value>
    </parameter>
    <parameter identifier="i">
      <param-name>パケット送信間隔（ミリ秒）</param-name>
      <param-type />
      <value>10</value>
    </parameter>
    <parameter identifier="b">
      <param-name>パケット送信時間（秒）</param-name>
      <param-type />
      <value>10</value>
    </parameter>
  </config>
  <config id="0009">
    <name>Ping of Death</name>
    <monitoring>
      <interval>1</interval>
      <after-count>5</after-count>
      <error-count>3</error-count>
    </monitoring>
    <parameter identifier="a">
      <param-name>送信元IPアドレス</param-name>
```

IPv6



4)-13.3. 詳細ログファイル

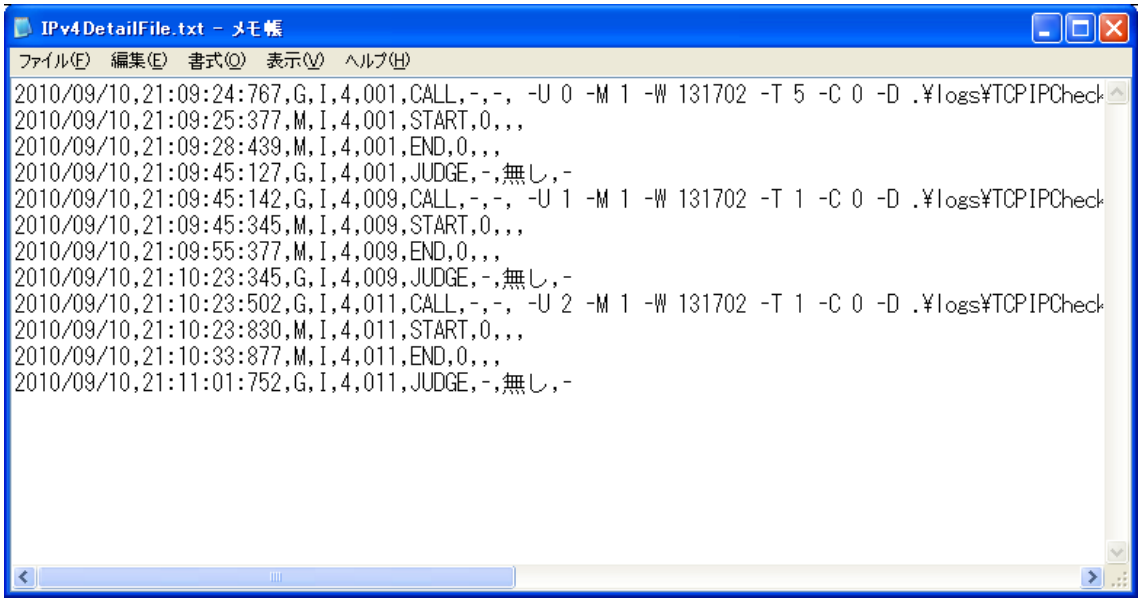
本ツールの稼働詳細ログファイルであり、ツールの起動/終了、各モジュールの起動・終了、脆弱性の有無判定時の情報や、エラー発生時の情報等を出力するファイルです。

詳細ログファイルは以下の内容で出力されます。形式はテキスト形式で、セパレータはカンマです。

日付,時刻,ツール識別子,ツール,プロトコル,モジュール ID,イベント,戻り値,脆弱性判定,パラメータ,付加情報

項目	説明
日付	ログが出力された日付、yy/mm/dd 形式で出力
時刻	ログが出力された時刻。HH:MM:SS:MMM 形式で出力
ツール識別子	ログを出力したのがどのツールなのかを表示する。以下の 2 パターンが存在する。 G：画面、 M：モジュール
ツール	検証ツールと確認ツールどちらで出力されたのか識別するためのパラメータ。以下の 2 パターンが存在する。 I：検証ツール C：確認ツール
プロトコル	IPv4 と IPv6 どちらで出力されたのか識別するためのパラメータ。以下の 2 パターンが存在する。 4：IPv4 6：IPv6
モジュール ID	プログラム番号の数字 3 桁を表示する。
イベント	詳細ログが書き込まれたイベントを表示する。検証ツールでは以下の 4 パターンが存在する。 CALL：画面側がモジュールを呼び出したイベント START：モジュールが起動したイベント END：モジュールが終了したイベント JUDGE：画面側が脆弱性を判断したイベント
戻り値	モジュールの終了コードを表示する。
脆弱性判定	脆弱性判定の結果を表示する。以下の 5 パターンが存在する。 －：ポートの監視を行わなかった際に表示される 無し：接続エラーが一度も起きなかった 有りの疑い：接続エラー回数が一回以上しきい値以下だった 検証エラー：対象ポートの監視が行えなかった 有り：接続エラー回数がしきい値以上だった
パラメータ	モジュール起動時のパラメータを表示する
付加情報	エラー及び脆弱性判定理由を表示する。

以下に詳細ログファイルのサンプルを記載します。



4)-13.4. 検証結果ファイル

脆弱性検証後の検証結果を出力するファイルです。

検証結果ファイルは以下の内容で出力されます。ファイルの形式は CSV 形式です。セパレータはカンマです。

日付,時刻,検証対象機器,脆弱性項目名,検証状況,送信パケット数,送信エラー数,監視エラー数,脆弱性判定

項目	説明
日付	脆弱性検証/確認が終了した日付。YYYY/MM/DD 形式で出力
時刻	脆弱性検証/確認が終了した時刻。　HH:MM:SS 形式で出力
検証対象機器	検証対象機器の IP アドレス
脆弱性項目名	対象脆弱性項目の番号と名称
検証状況	検証状況が出力されます。以下の 7 パターンが存在します －：まだ検証が実行されていません 検証中：検証を行っています 監視中：サービスの監視を行っています 検証エラー：攻撃パケットの送信処理において、エラーが発生しま

	した 中止：検証が中止されました スキップ：検証が実施されることなく、スキップされました 完了：検証が終了いたしました
送信パケット数	検証モジュールが送信したパケット数
送信エラー数	検証モジュールのパケット送信エラー数
監視エラー数	検証モジュール実行終了後のサービス監視でポート接続エラー数
脆弱性判定	脆弱性判定の結果が表示されます。以下の 5 つのパターンが存在します。 －：ポートの監視を行わなかった際に表示 無し：接続エラーが一度も起きなかった 有りの疑い：接続エラー回数が一回以上しきい値以下だった 検証エラー：対象ポートの監視が行えなかった 有り：接続エラー回数がしきい値以上だった

以下に検証結果ファイルのサンプルを記載します。

4)-13.5. 設定ファイル

設定ファイルは、コマンドラインでツールを稼働させるときに必要なパラメータが記載されているファイルです。形式は ini ファイルです。

設定ファイルの作成を行う時、下記表を参考に新規に作成を行うか、以下のフォルダ内に存在するサンプルファイルを編集することで作成を行ってください。設定ファイルの作成はサンプルファイルをコピーし、編集して作成することを推奨します。

IPv4

<インストールディレクトリ>¥サンプル¥IPv4¥IPv4.ini

IPv6

<インストールディレクトリ>¥サンプル¥IPv6¥IPv6.ini

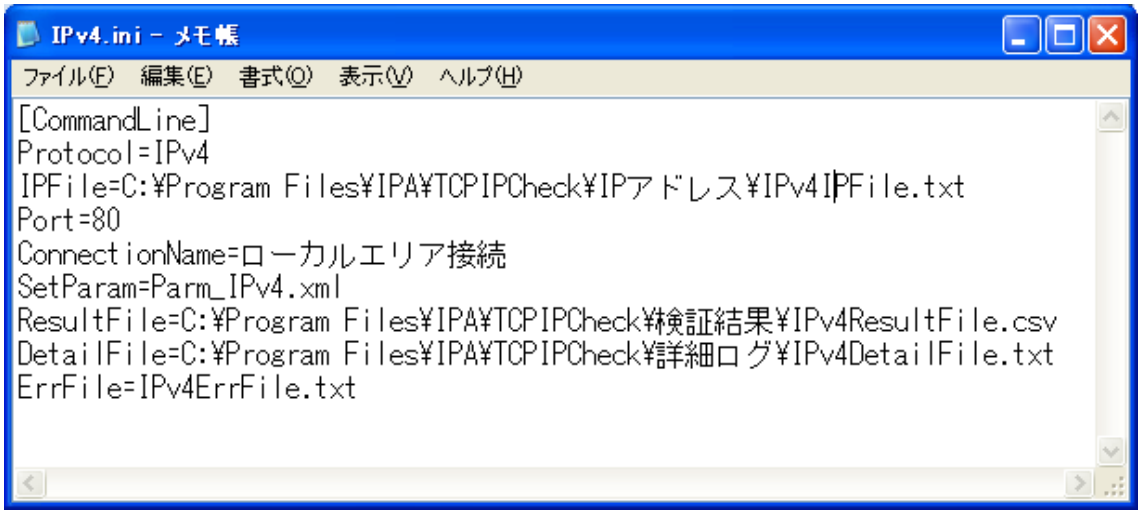
パラメータ名	説明	必須
[CommandLine]	セクション。[CommandLine]で固定。	●
Protocol	IPv4,で検証する時は IPv4、 IPv6 で検証する時は IPv6 と入力します。	●
IPFile	検証対象が記載されている IP アドレスファイル名を記入します。指定するファイルは[4)-13.1]に則ったものにしてください。	●
Port	監視ポート番号を指定します。指定しなかった時、ポートの監視は行われません。	○
ConnectionName	使用するネットワーク接続名を指定します。 入力値は、脆弱性選択画面で使用するネットワーク接続名を選択後、[コピー]ボタンをクリックしてクリップボードに張り付けられたものを使用することで、簡単に設定できます。	●
SetParam	検証に使用するパラメータが記載されているパラメータファイル名を記入します。指定するファイルは[4)-13.2]に則ったものにしてください。	●
ResultFile	検証結果の出力先となるファイル名を記入します。出力されるファイルの形式は、[4)-13.4]に則ったものになります	●
DetailFile	詳細ログの出力ファイルを指定します。出力されるファイルの形式は、[4)-13.3]に則ったものになります。指定しなかった時、詳細ログの出力は行われません。	○
ErrFile	エラーログの出力ファイルを指定します。出力されるファイルの形式は、[4)-13.6]に則ったものになります 未指定の時、本ツールのインストールフォルダ¥ TCPIP_Err.log”をデフォルトとして使用します。	○

● 必須

○ 任意

設定ファイルで使用するファイル名は、絶対パスを指定したファイル名、もしくはファイル名のみとし、相対パスを使用しないでください。また、ファイルの内容は大文字と小文字が区別されません。

以下に設定ファイルのサンプルを記載します。



4)-13.6. エラーログファイルの書式

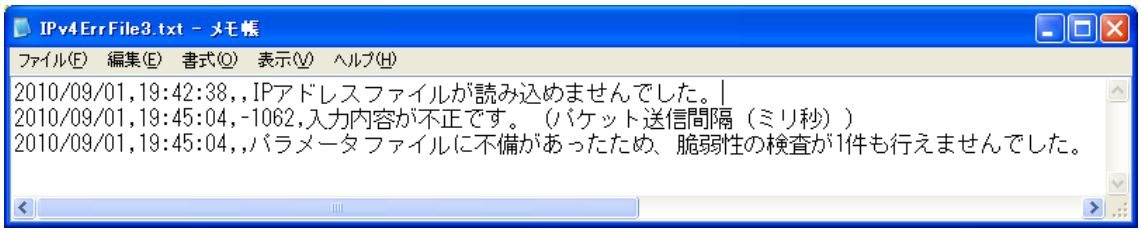
コマンドライン起動時に、何らかのエラーが発生した時にエラー内容が出力されるファイルです。エラーファイルには、以下の内容で出力されます。セパレータはカンマです。

日付,時刻,戻り値,エラーメッセージ

項目	説明
日付	エラーが発生した日付、YYYY/MM/DD 形式で出力します。
時刻	エラーが発生した時刻、 HH:MM:SS 形式で出力します。
戻り値	検証モジュールでエラーが発生した時、モジュールの戻り値を出力します。
エラーメッセージ	どのようなエラーが発生したのか、その内容について出力します。詳細については[4)-12]も参照してください。

なお、設定ファイルの読み込みに関わるエラーが発生した時、エラーログファイルにエラーは書き込まれません。設定ファイルに関わるエラーの確認はイベントログを参照してください。

以下にエラーログのサンプルを記載します。



5). 項目別検証方法

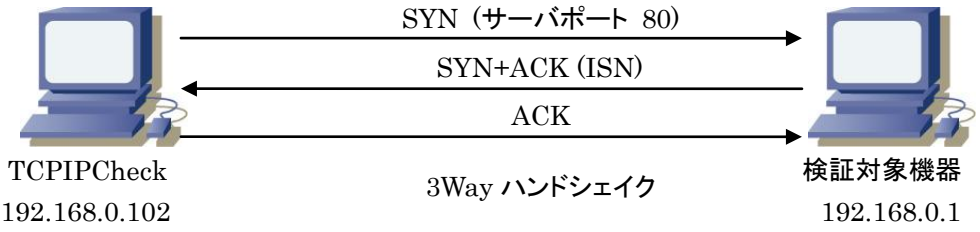
5)-1.TCP ISN 予測

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

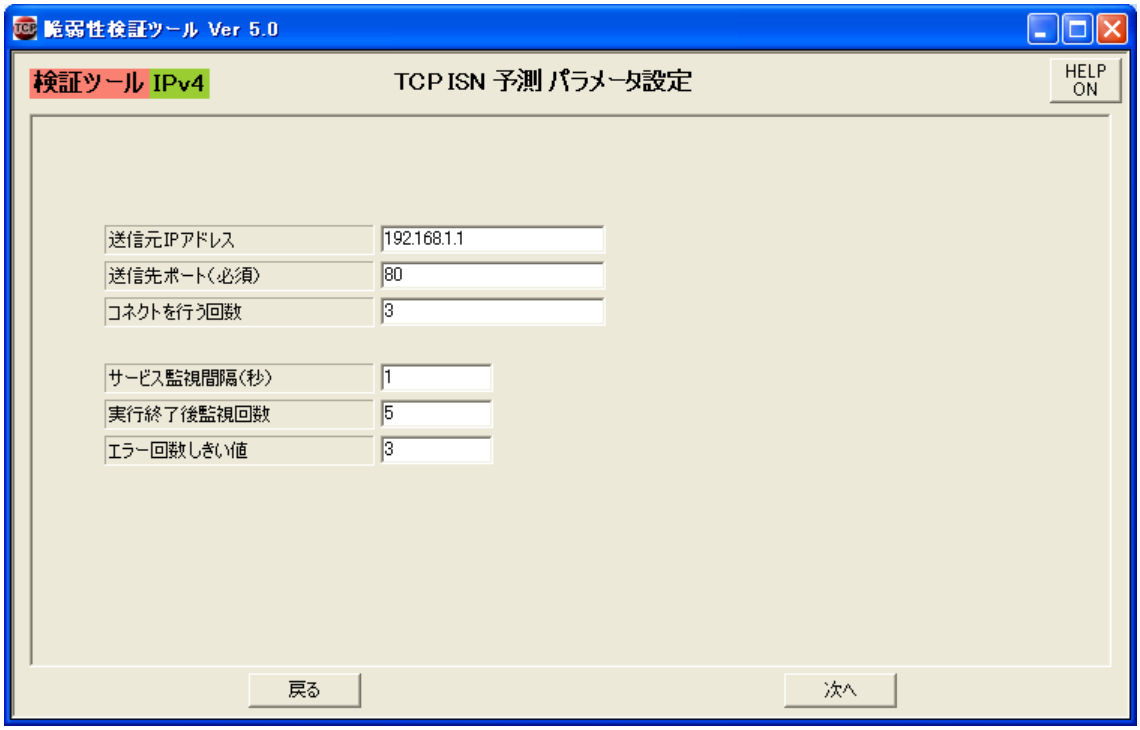
参照：1) TCP の初期シーケンス番号予測の問題

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

TCP のセッション確立の際に検証対象機器から通知される ISN(Initial Sequence Number：初期シーケンス番号)を解析し、規則性の有無を調査します。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。 CLOSE 状態のポート番号を指定すると、検証対象から Reset パケットが送信されるだけで、ISN の規則性を調査することができません。
コネクトを行う回数	3

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

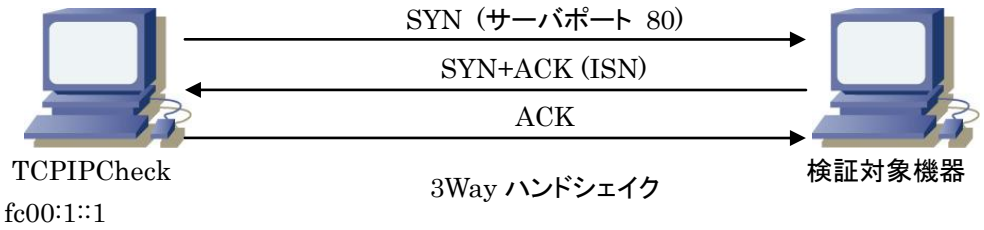
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

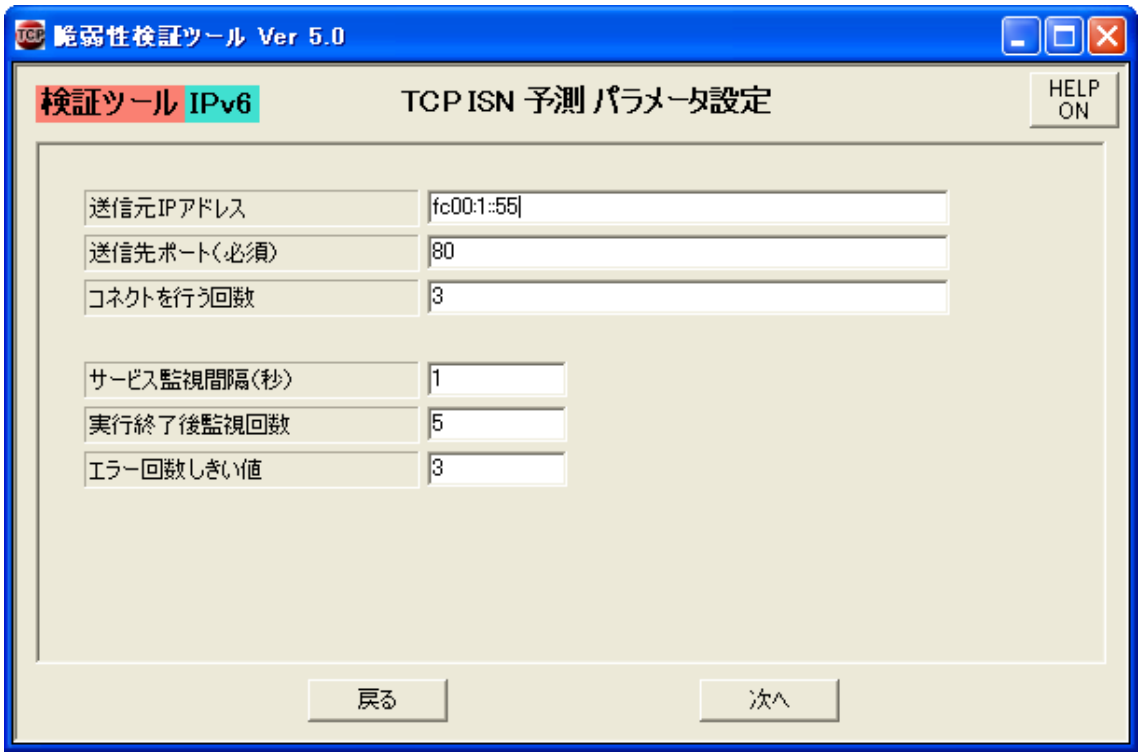
- 脆弱性検証確認画面の脆弱性判定を確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

TCP のセッション確立の際に検証対象機器から通知される ISN を解析し、規則性の有無を調査します。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。 CLOSE 状態のポート番号を指定すると、検証対象から Reset パケットが送信されるだけで、ISN の規則性を調査することができません。
コネクトを行う回数	3

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 脆弱性検証確認画面の脆弱性判定を確認してください。

5)-2.[未実装]TCP 接続の強制切断の問題

未実装

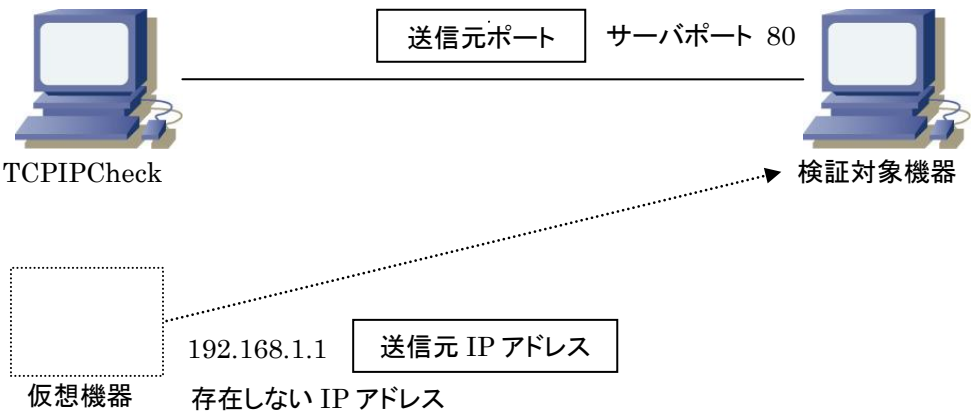
5)-3.SYN Flood

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

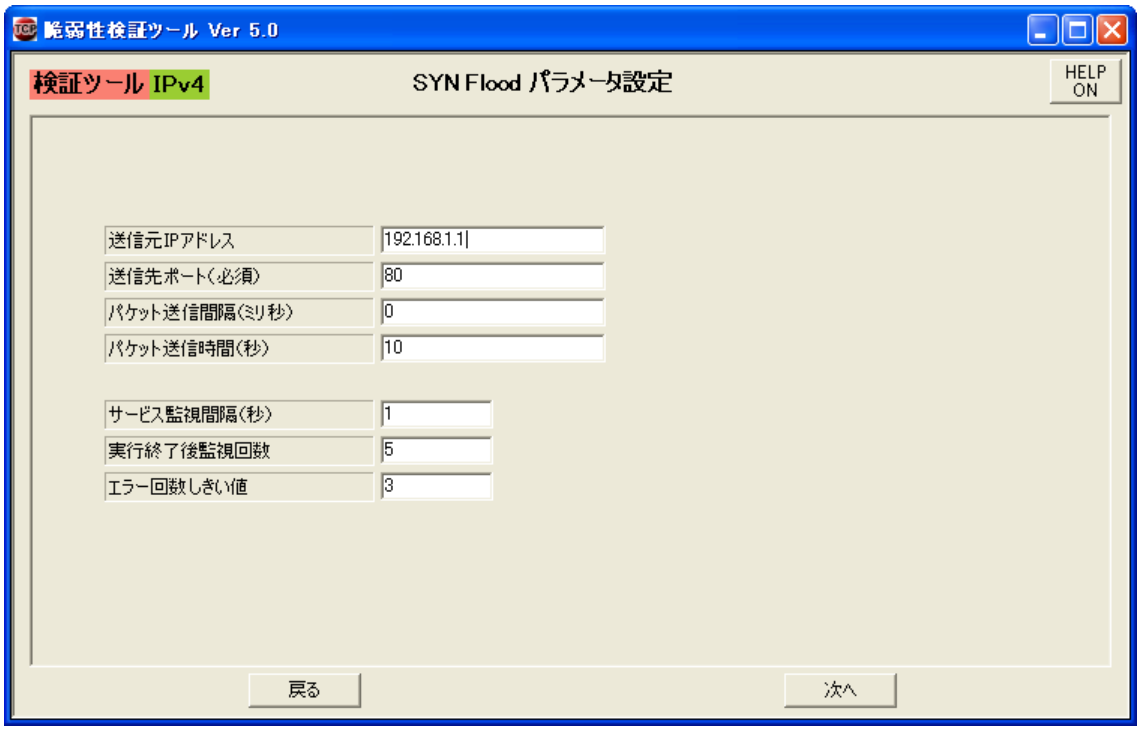
参照：3) SYN パケットにサーバ資源が占有される問題（SYN Flood Attack）

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

TCP の SYN パケットを送信します。検証対象機器に、完了待ちの接続を大量に持たせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	存在しない（通信不能である）IP アドレスを指定してください。 存在する IP アドレスを指定すると、その機器から Reset パケットが検証対象に送信されて、効果がなくなる可能性があります。
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。 CLOSE 状態のポート番号を指定すると、検証対象から Reset パケットが送信されるだけで、効果がありません。
パケット送信間隔	0
パケット送信時間	検証対象機器の性能により異なるので、共通の推奨値はありません(最大指定可能値は 100 万秒です)。

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

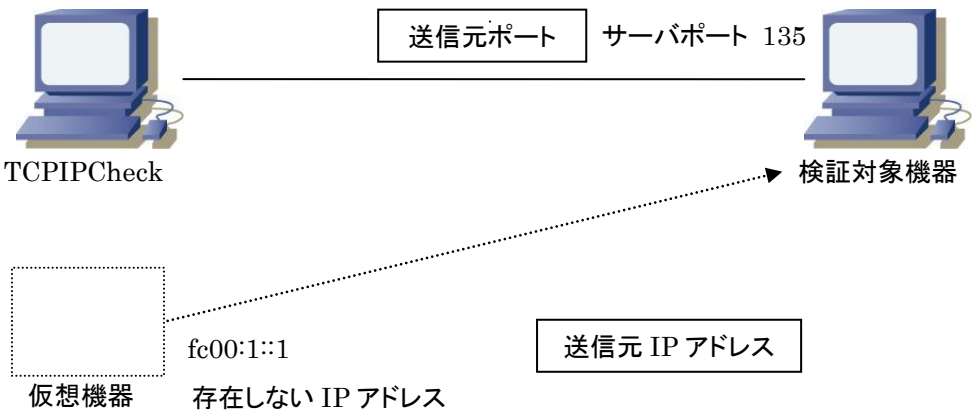
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面

攻撃パケットの概要

TCP の SYN パケットを送信します。検証対象機器に、完了待ちの接続を大量に持たせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	存在しない（通信不能である）IP アドレスを指定してください。 存在する IP アドレスを指定すると、その機器から Reset パケットが検証対象に送信されて、効果がなくなる可能性があります。
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。 CLOSE 状態のポート番号を指定すると、検証対象から Reset パケットが送信されるだけで、効果がありません。
パケット送信間隔	0
パケット送信時間	検証対象機器の性能により異なるので、共通的な推奨値はありません(最大指定可能値は 100 万秒です)。

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

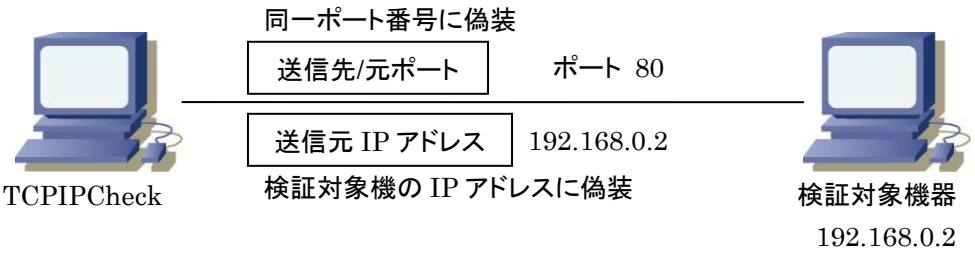
5)-4.LAND Attack

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

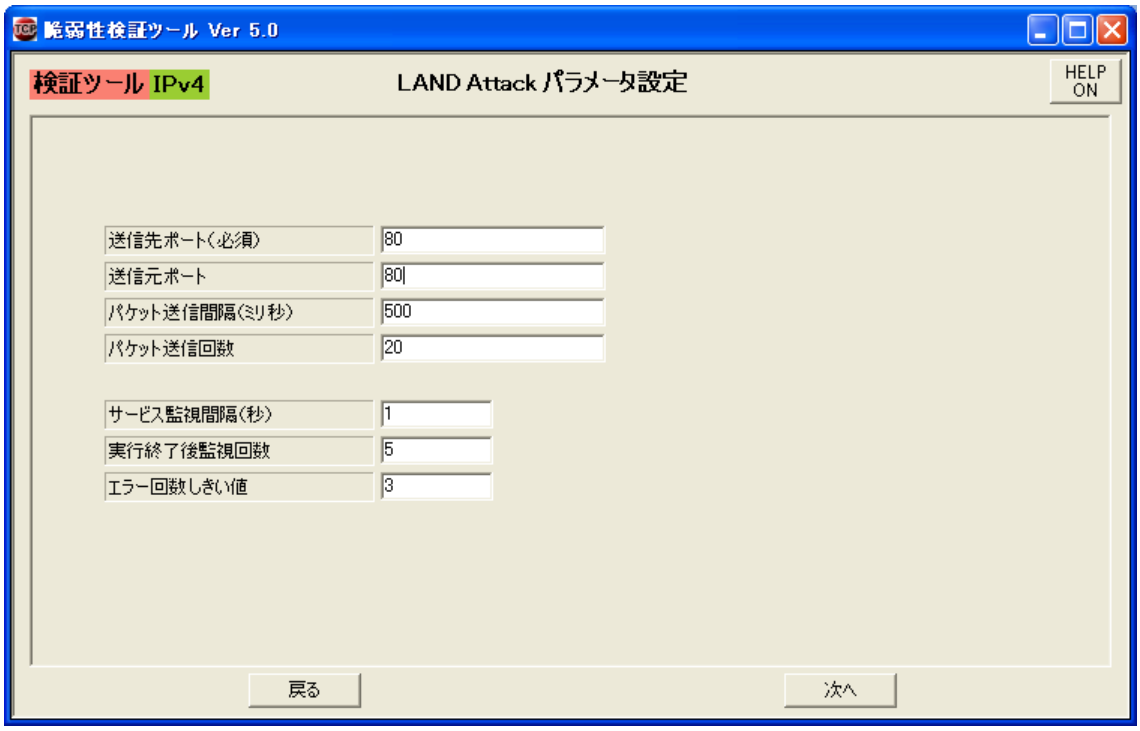
参照：4) 特別な SYN パケットによりカーネルがハングアップする問題（LAND Attack）

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

送信先、送信元 IP アドレスを同一にした SYN パケットを送信することで SYN/ACK パケットを自分自身に送信させ、システム資源を枯渇させたり、カーネルをハングアップさせたりすることが狙いです。

この時、送信先、送信元ポート番号を同一にすることにより効果がある時もあります。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。
送信元ポート	送信先ポートと同一の値にすると効果が得られる時があります。
パケット送信間隔	500
パケット送信回数	20

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

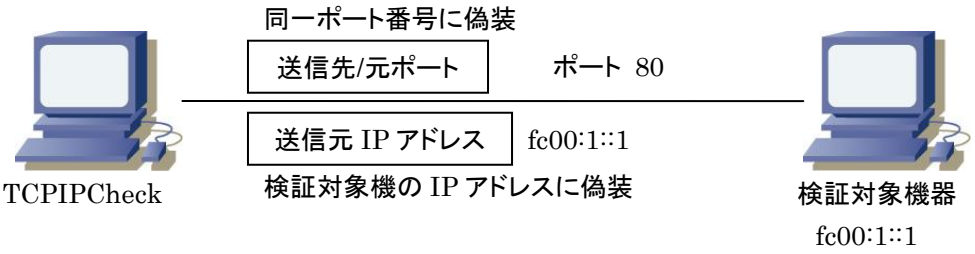
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面

攻撃パケットの概要

送信先、送信元 IP アドレスを同一にした SYN パケットを送信することで SYN/ACK パケットを自分自身に送信させ、システム資源を枯渇させたり、カーネルをハングアップさせたりすることが狙いです。

この時、送信先、送信元ポート番号を同一にすることにより効果がある時もあります。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。
送信元ポート	送信先ポートと同一の値にすると効果が得られる時があります。
パケット送信間隔	500
パケット送信回数	20

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

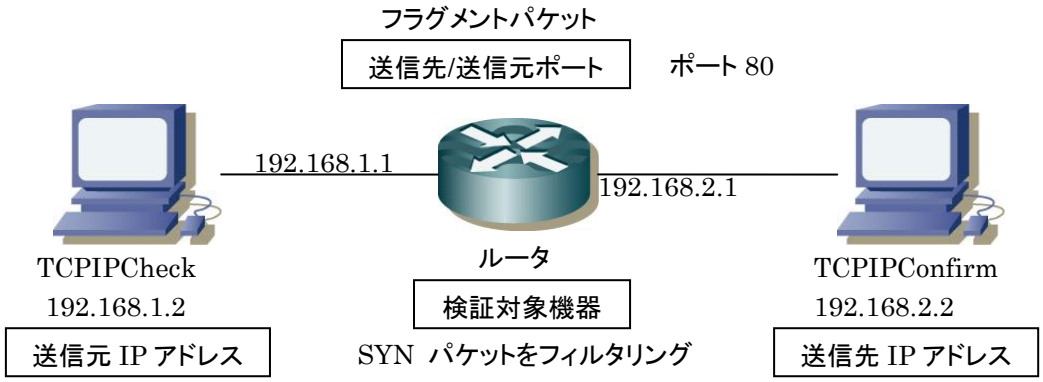
5)-5.Overlapping Fragment

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

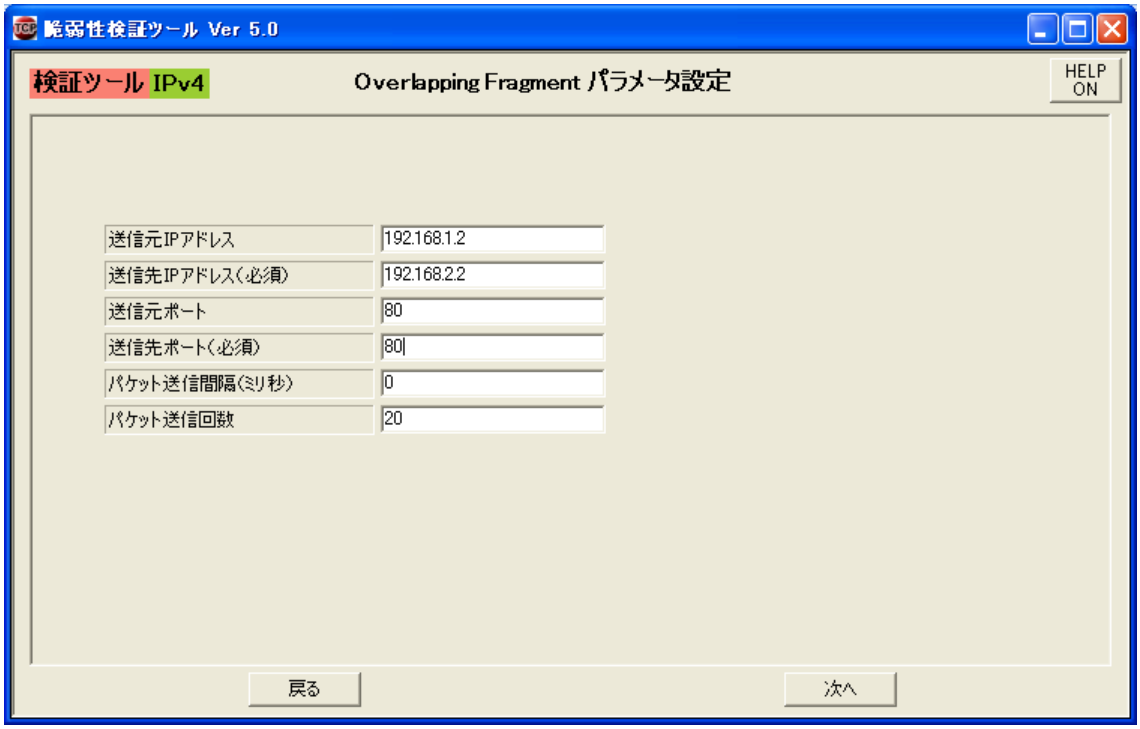
参照：5) データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題（Overlapping Fragment Attack）

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

TCP パケットを一部重複する形でフラグメント化し、本来はフィルタリングを設定しているため通過できないはずのルータを通過させる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先 IP アドレス	検証対象機器（ルータ）の先にある通信可能な機器の IP アドレスを指定してください。 TCPIPConfirm ツール(IPv4)を使用する時は、TCPIPConfirm ツール(IPv4)のパラメータ設定画面に表示される"送信元 IP アドレス"を指定してください。
送信先ポート	検証対象の OPEN 状態の TCP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	0
パケット送信回数	20

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

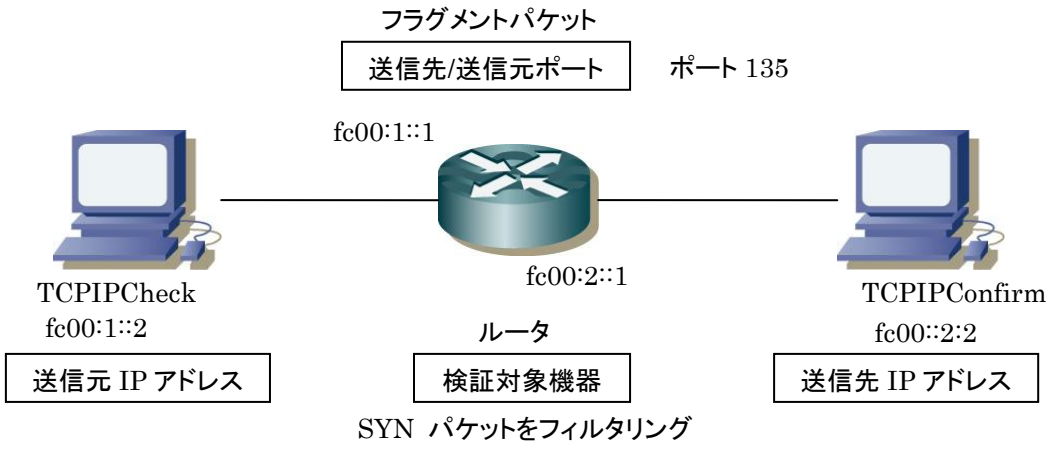
以下のような方法で、脆弱性有無の確認を行ってください。

- 送信先 IP アドレスで指定した機器で TCPIPConfirm ツール(IPv4)を起動し、パケットが到達していないか確認してください。

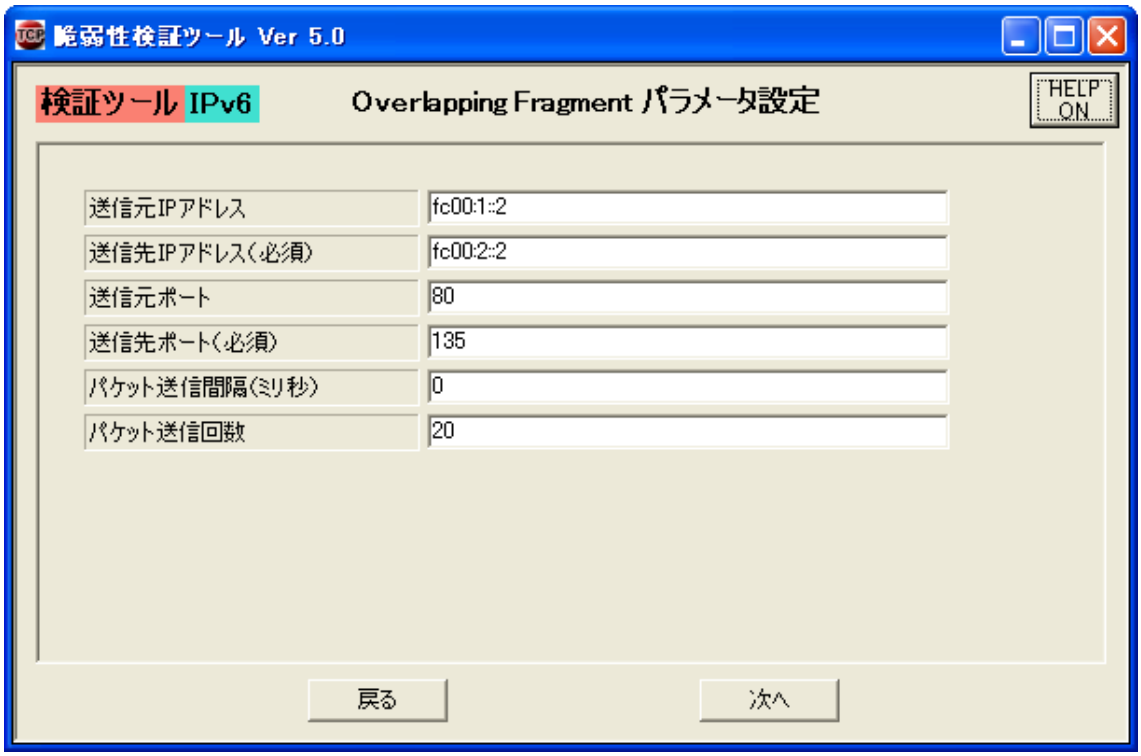
[IPv6]

[重要]この検証はユニークローカルユニキャストアドレスが正しく設定されていないネットワーク環境では正常に機能しません。

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

TCP パケットを一部重複する形でフラグメント化し、本来はフィルタリングを設定しているため通過できないはずのルータを通過させる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先 IP アドレス	検証対象機器（ルータ）の先にある通信可能な機器の IP アドレスを指定してください。 TCPIPConfirm ツール(IPv6)を使用する時は、TCPIPConfirm ツール(IPv6)のパラメータ設定画面に表示される"送信元 IP アドレス"を指定してください。
送信先ポート	検証対象の OPEN 状態の TCP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	0
パケット送信回数	20

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 送信先 IP アドレスで指定した機器で TCPIPConfirm ツール(IPv6)を起動し、パケットが到達していないか確認してください。

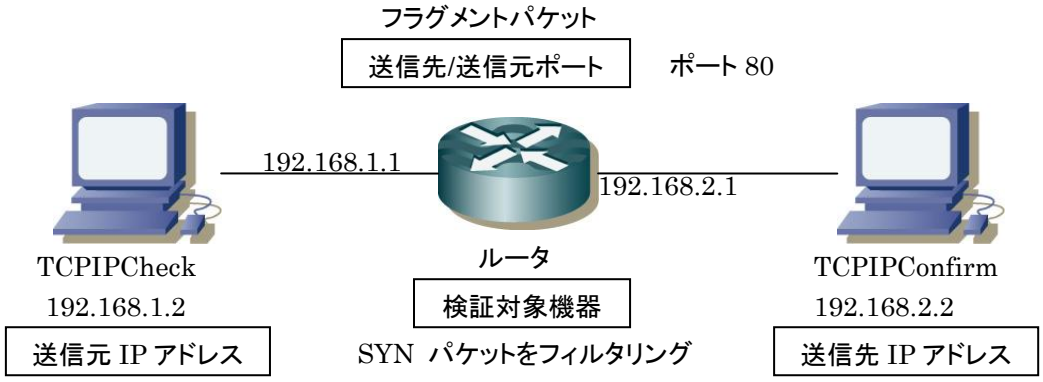
5)-6.Tiny Fragment

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：6) 十分に小さい分割パケットがフィルタリングをすり抜ける問題　(Tiny Fragment Attack、Tiny Overlapping Fragment Attack)

[IPv4]

ネットワーク構成の例



パラメータ設定画面

攻撃パケットの概要

TCP の第一フラグメントパケットを 8 オクテットとし、制御フラグを第二フラグメントパケットに含める事により、第一フラグメントパケットのみを注目しているフィルタリングを通過させる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先 IP アドレス	検証対象機器（ルータ）の先にある通信可能な機器の IP アドレスを指定してください。 TCPIPConfirm ツール(IPv4)を使用する時は、TCPIPConfirm ツール(IPv4)のパラメータ設定画面(P.75)に表示される"送信元 IP アドレス"を指定してください。
送信先ポート	検証対象の OPEN 状態の TCP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	0
パケット送信回数	20

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

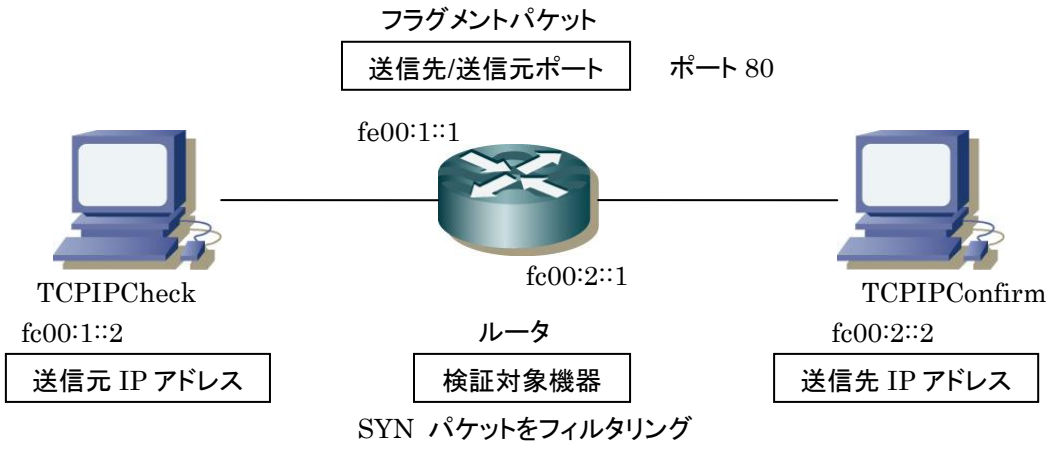
以下のような方法で、脆弱性有無の確認を行ってください。

- 送信先 IP アドレスで指定した機器で TCPIPConfirm ツール(IPv4)を起動し、パケットが到達していないか確認してください。

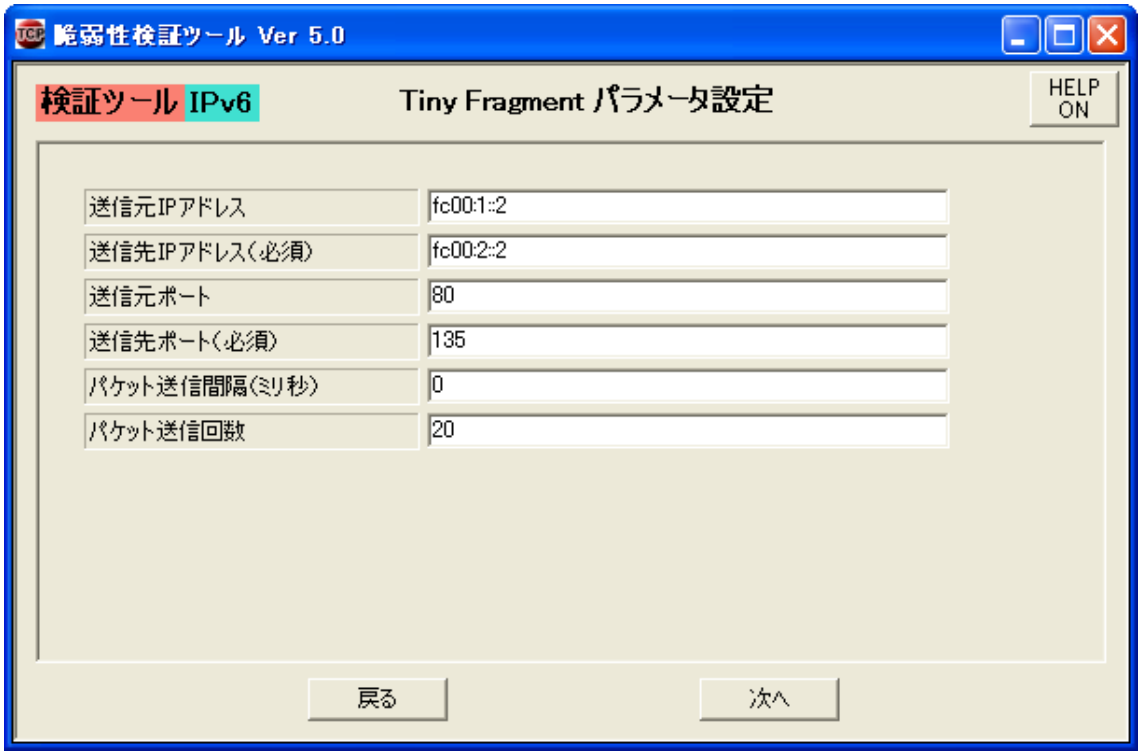
[IPv6]

[重要]この検証はユニークローカルユニキャストアドレスが正しく設定されていないネットワーク環境では正常に機能しません。

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

TCP の第一フラグメントパケットを 8 オクテットとし、制御フラグを第二フラグメントパケットに含める事により、第一フラグメントパケットのみを注目しているフィルタリングを通過させる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先 IP アドレス	検証対象機器（ルータ）の先にある通信可能な機器の IP アドレスを指定してください。 TCPIPConfirm ツール(IPv6)を使用する時は、TCPIPConfirm ツール(IPv6)のパラメータ設定画面(P.76)に表示される"送信元 IP アドレス"を指定してください。
送信先ポート	検証対象の OPEN 状態の TCP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	0
パケット送信回数	20

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 送信先 IP アドレスで指定した機器で TCPIPConfirm ツール(IPv6)を起動し、パケットが到達していないか確認してください。

5)-7.[未実装]PAWS 機能の内部タイマを不正に更新することで、TCP 通信が強制的に切断される問題

未実装

5)-8.[未実装]Optimistic TCP acknowledgements により、サービス不能状態に陥る問題

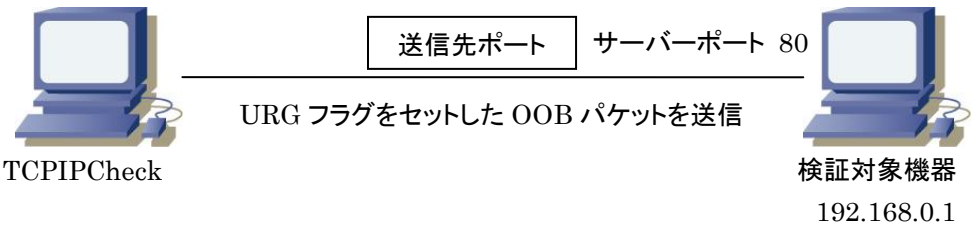
未実装

5)-9.Out Of Band

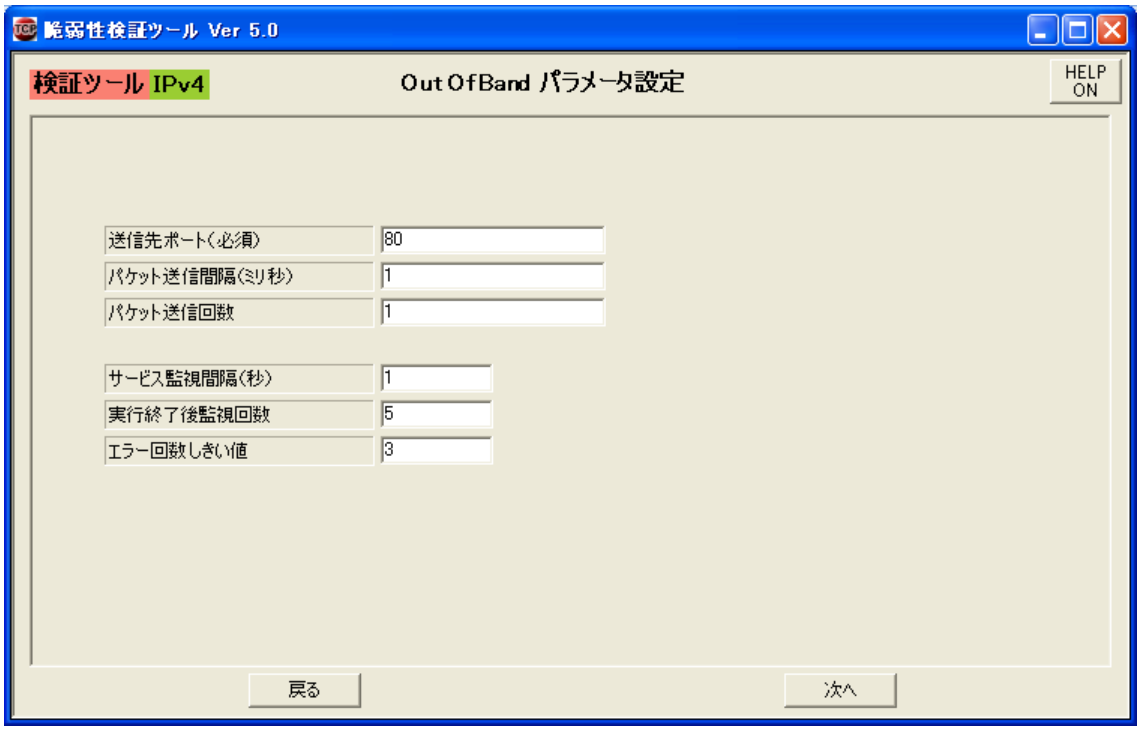
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：9) Out Of Band(OOB)パケットにより、サービス不能状態に陥る問題

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

URG フラグをセットした Out Of Band(OOB)パケットを送信し、検証対象機器のアプリケーションまたは OS を異常終了させることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信先ポート	検証対象の OPEN 状態のポート番号を指定してください。
パケット送信間隔	1
パケット送信回数	1

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、動作が正常か確認してください。

5)-10.[未実装]ウインドウサイズ 0 の TCP 接続過多により、サービス不能状態に陥る問題

未実装

5)-11.[未実装]TCP 接続状態を操作し維持させることにより、サービス不能状態に陥る問題(Naptha Attack)

未実装

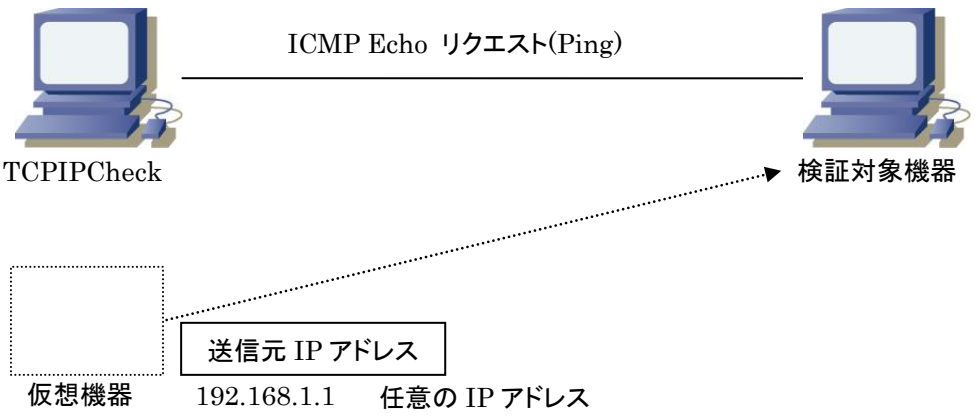
5)-12.Ping of Death

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

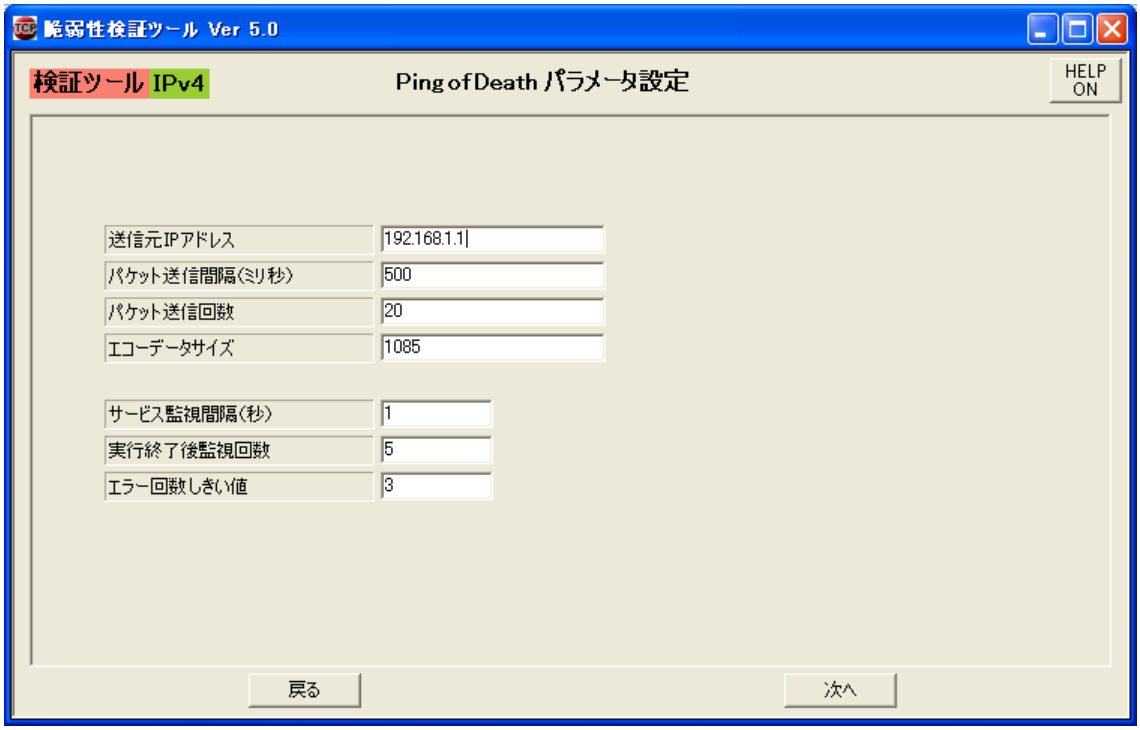
参照：12)パケット再構築時にバッファが溢れる問題（Ping of Death）

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

フラグメント化された ICMP Echo リクエスト(Ping)を送信し、検証対象機器においてパケットを再構築する際にバッファオーバーフローを発生させ、システムクラッシュやリブートをさせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
パケット送信間隔	500
パケット送信回数	20
エコーデータサイズ	1085

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

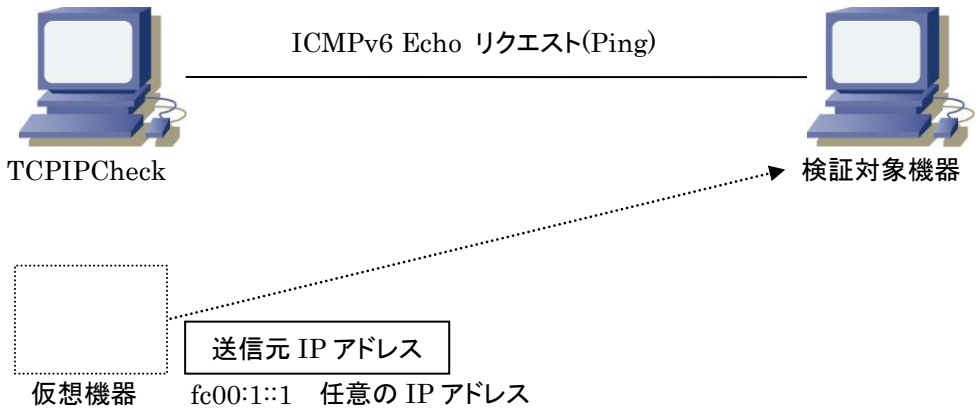
- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してく

ださい。

- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面

攻撃パケットの概要

フラグメント化された ICMPv6 Echo リクエスト(Ping)を送信し、検証対象機器においてパケットを再構築する際にバッファオーバーフローを発生させ、システムクラッシュやリブートをさせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
エコーデータサイズ	1085
パケット送信間隔	500
パケット送信回数	20

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

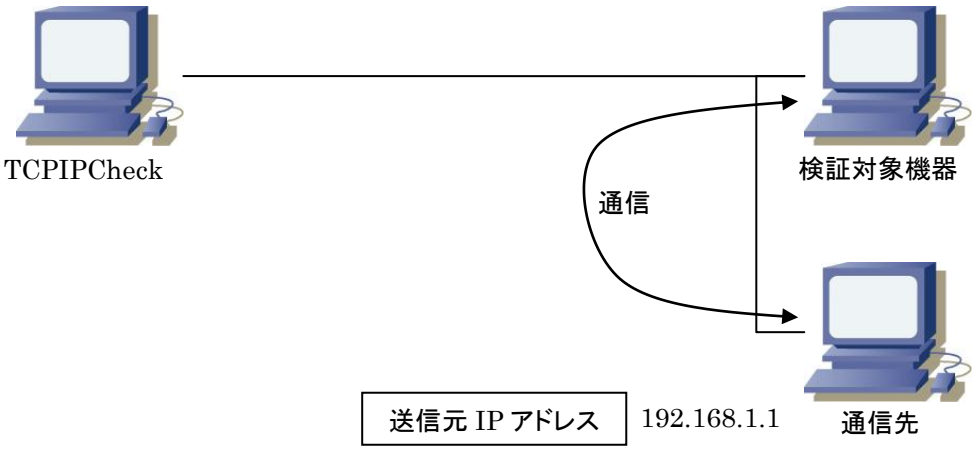
5)-13.Path MTU Discovery

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

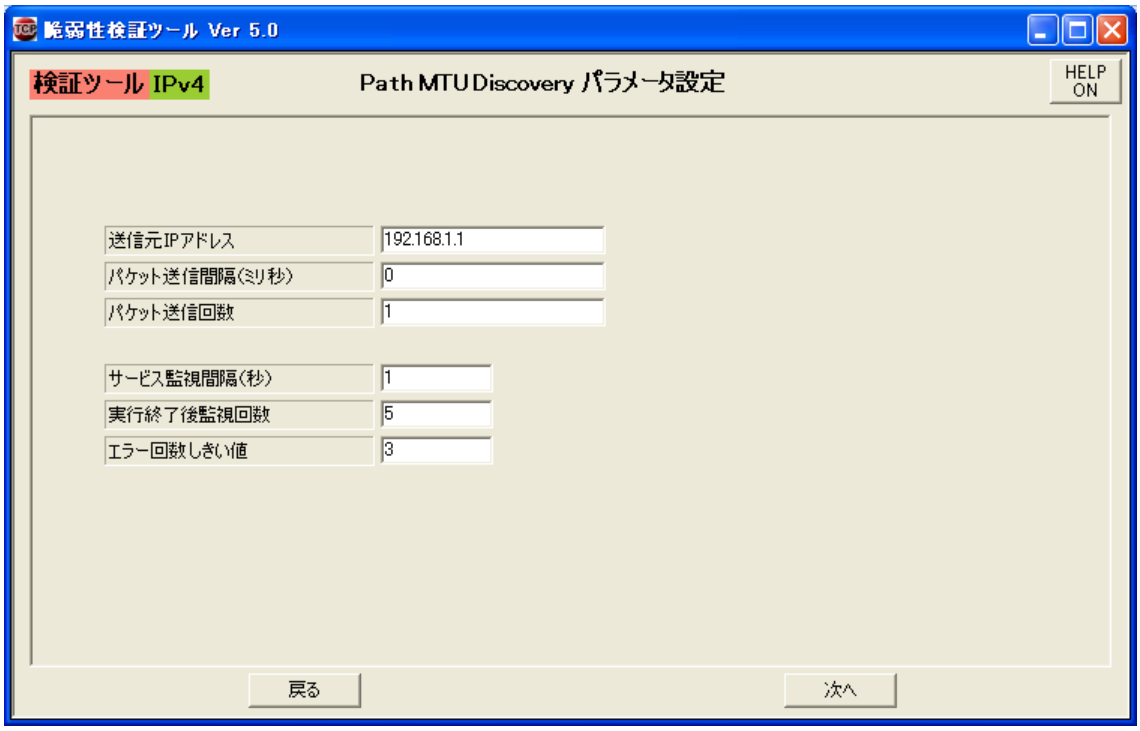
参照：12) ICMP Path MTU Discovery 機能を利用した通信遅延の問題

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP Path MTU Discovery パケットを送信して、検証対象機器に極度に小さな MTU を設定させ、通信スループットを低下させることが狙いです。この攻撃では MTU を 68 にします。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が実際に通信を行っている機器の IP アドレスを指定してください。
パケット送信間隔	0
パケット送信回数	1

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

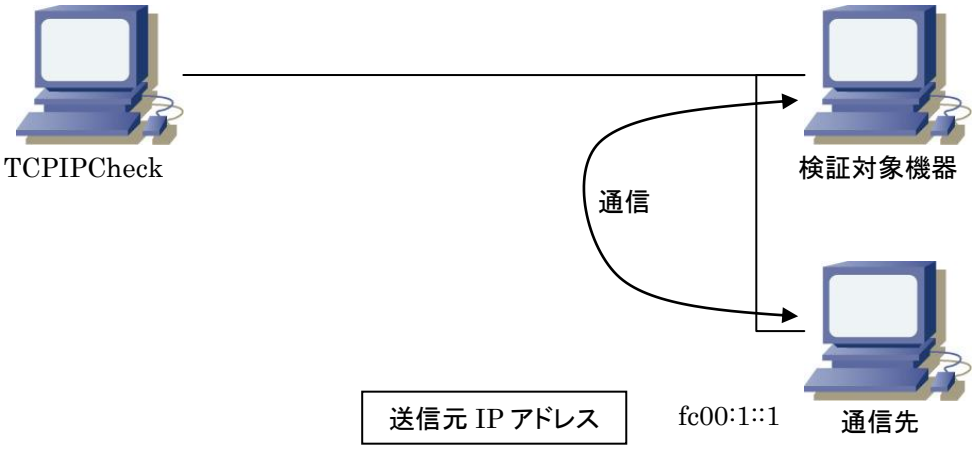
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

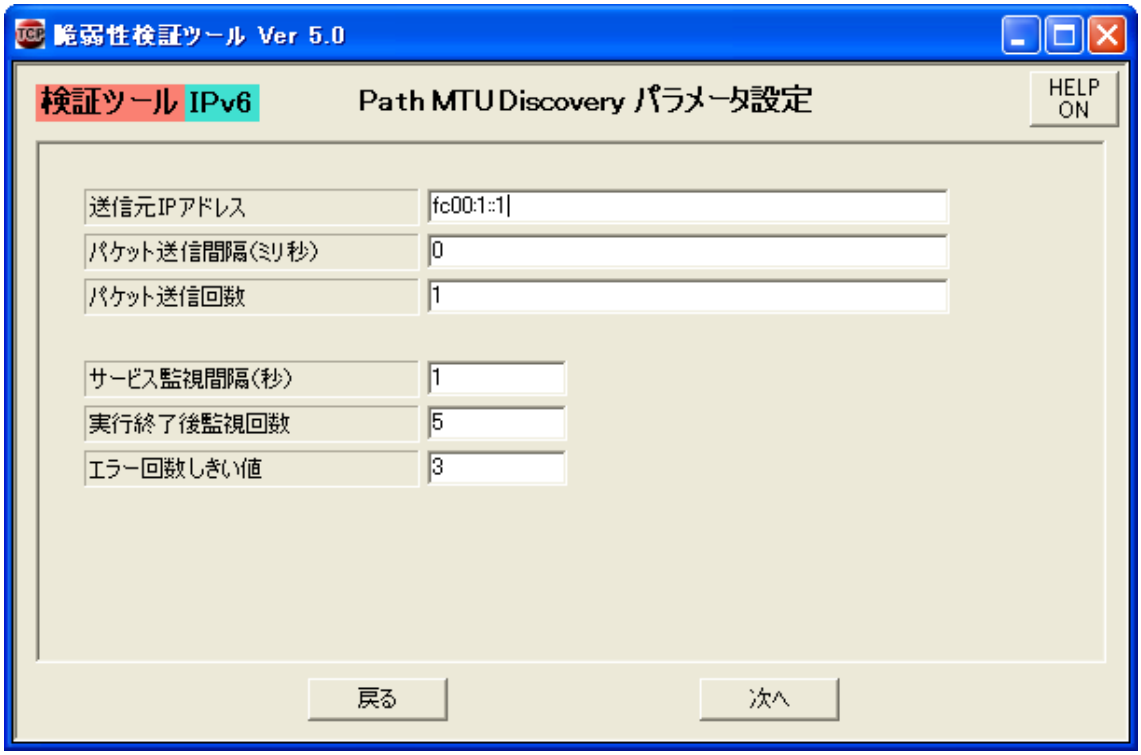
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。パケットキャプチャを行って、攻撃後にパケットサイズが小さくなっていれば確実に脆弱性があります。効果があるのは、検証対象から出力されるパケットのみです。

[IPv6]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP Path MTU Discovery パケット(IPv6 は Packet too big パケット)を送信して、検証対象機器に極度に小さな MTU を設定させ、通信スループットを低下させることが狙いです。この攻撃では MTU を 68 にします。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が実際に通信を行っている機器の IP アドレスを指定してください。
パケット送信間隔	0
パケット送信回数	1

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。パケットキャプチャを行って、攻撃後にパケットサイズが小さくなっていれば確実に脆弱性があります。効果があるのは、検証対象から出力されるパケットのみです。

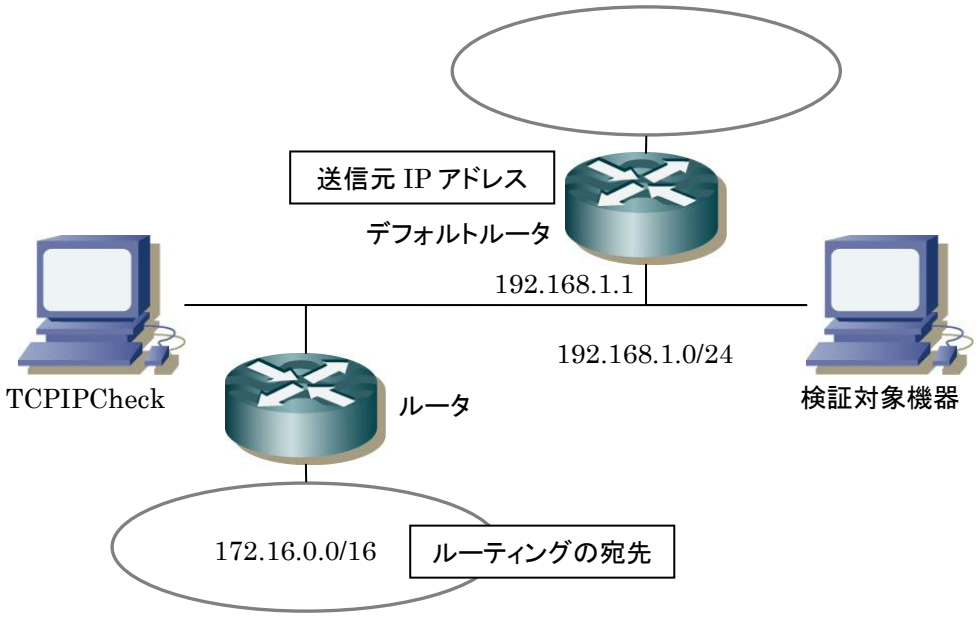
5)-14.ICMP Redirect DoS

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

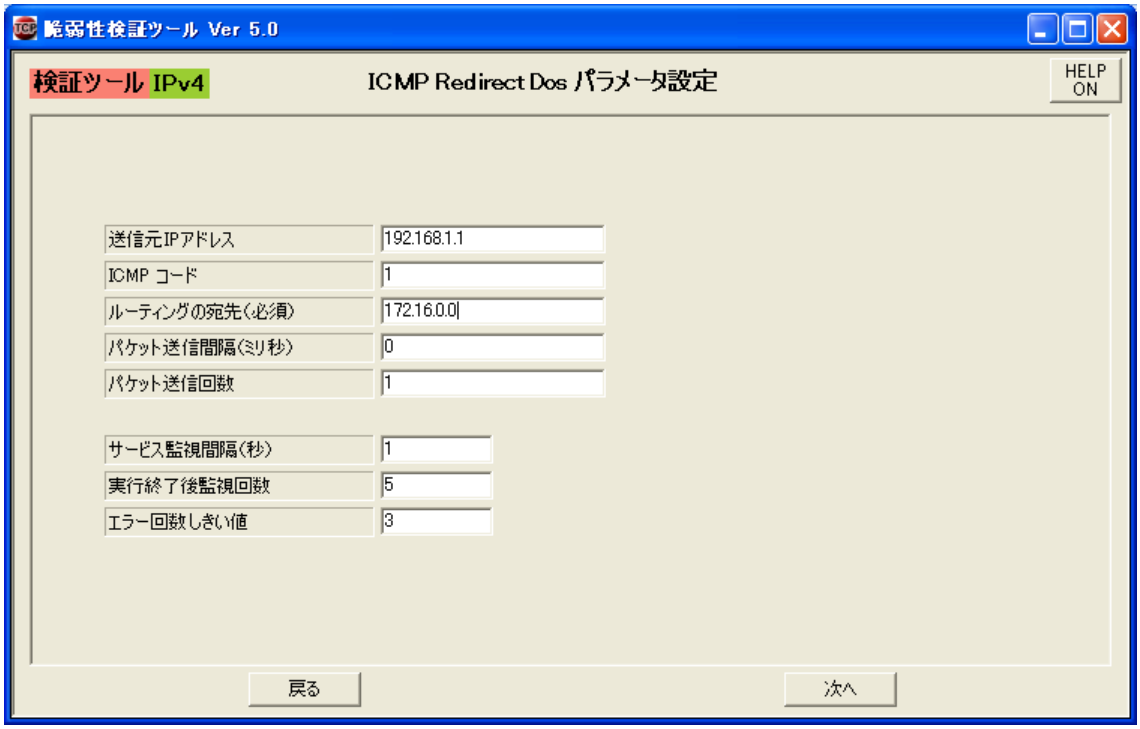
参照：14) ICMP リダイレクトによるサービス応答遅延の問題

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP Redirect パケットを送信して、検証対象機器のルーティングテーブルを書き換え、 送信先に自分自身を登録させて通信を妨害させることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が既に設定済みのゲートウェイ機器の IP アドレスを指定します。これは、検証対象が ICMP Redirect パケットを受け入れる確率を高くします。
ICMP コード	0 ネットワークに関するルート変更 1 ホストに関するルート変更 2 TOS とネットワークに関するルート変更 3 ホストと TOS に関するルート変更 すべての値でテストすることをお勧めします。
ルーティングの宛先	通信を妨害させるホストの IP アドレス、または、ネットワークの IP アドレスを指定します。
パケット送信間隔	0
パケット送信回数	1

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

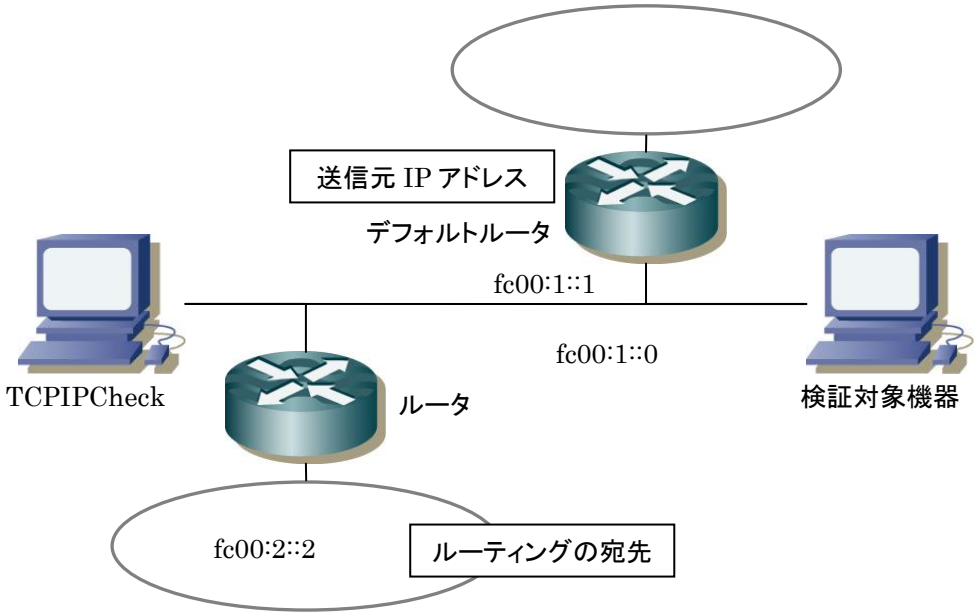
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- ルーティングの宛先で指定したホスト、または、ネットワークに対する通信ができなくなっていないか確認してください。
- 可能であれば、検証対象のルーティングテーブルを確認して、自分自身がゲートウェイとなっているエントリがないか確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面

攻撃パケットの概要

偽装した ICMP Redirect パケットを送信して、検証対象機器のルーティングテーブルを書き換え、　送信先に自分自身を登録させて通信を妨害させることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が既に設定済みのゲートウェイ機器の IP アドレスを指定します。これは、検証対象が ICMP Redirect パケットを受け入れる確率を高くします。
ルーティングの宛先	通信を妨害させるホストの IP アドレス、または、ネットワークの IP アドレスを指定します。
パケット送信間隔	0
パケット送信回数	1

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- ルーティングの宛先で指定したホスト、または、ネットワークに対する通信ができなくなっていないか確認してください。
- 可能であれば、検証対象のルーティングテーブルを確認して、自分自身がゲートウェイとなっているエントリがないか確認してください。

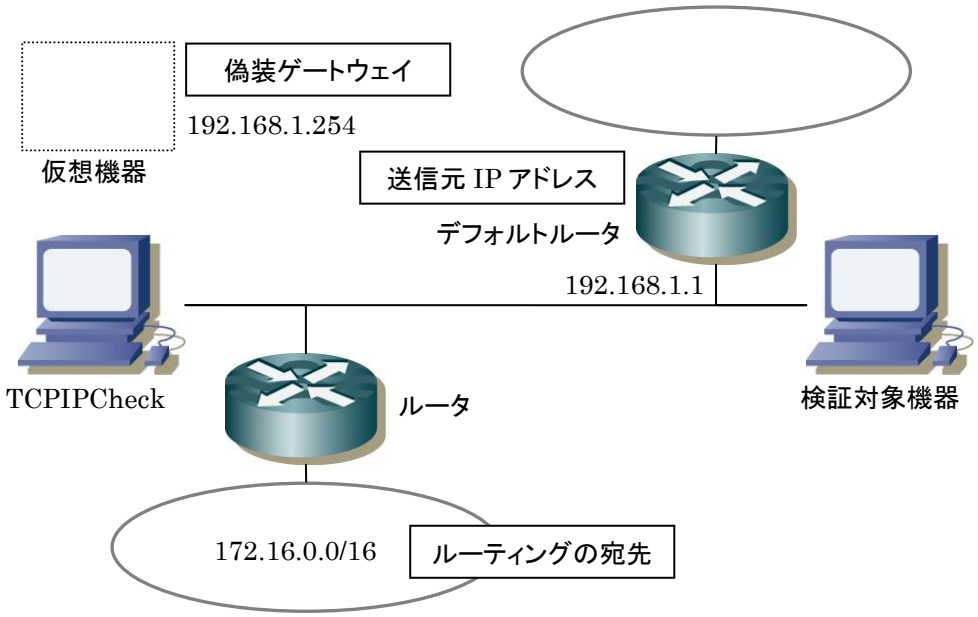
5)-15.ICMP Redirect Spoofing

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

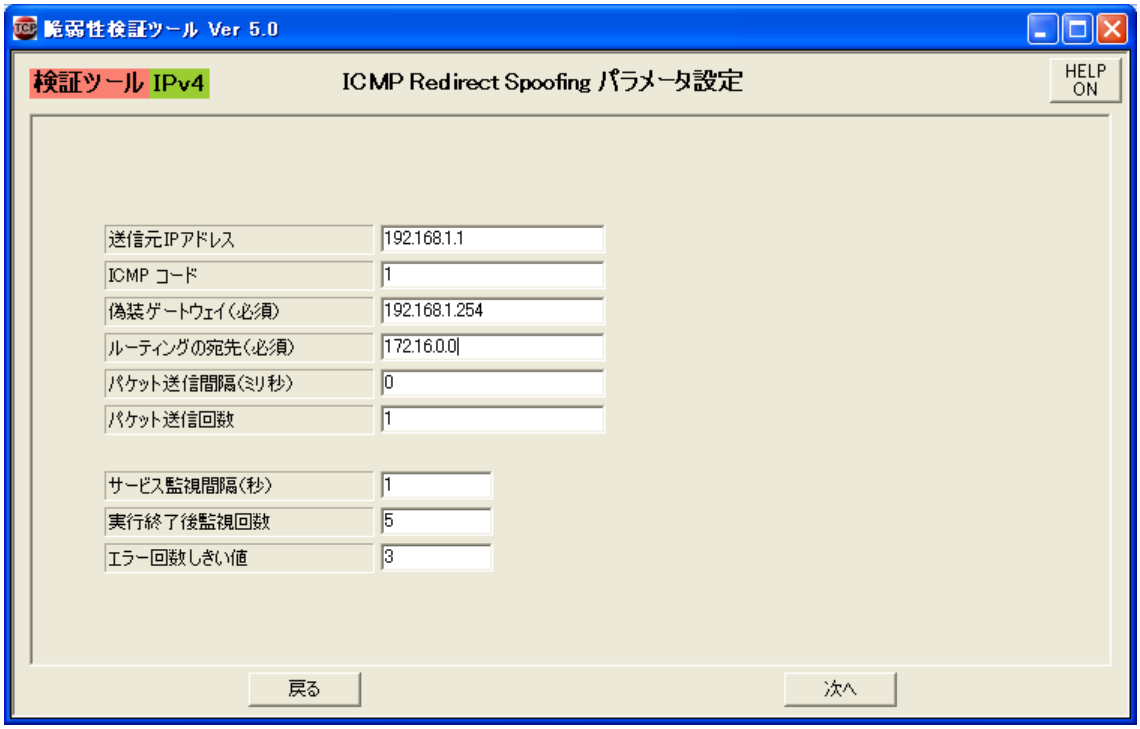
参照：15) ICMP リダイレクトによる送信元詐称の問題

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP Redirect パケットを送信して、検証対象機器のルーティングテーブルを書き換え、送信先に攻撃者の IP アドレスを登録させることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が既に設定済みのゲートウェイ機器の IP アドレスを指定します。これは、検証対象が ICMP Redirect パケットを受け入れる確率を高くします。
ICMP コード	0 ネットワークに関するルート変更 1 ホストに関するルート変更 2 TOS とネットワークに関するルート変更 3 ホストと TOS に関するルート変更 すべての値でテストすることをお勧めします。
偽装ゲートウェイ	検証対象機器と同一ネットワーク内の任意の IP アドレス。
ルーティングの宛先	通信を妨害させるホストの IP アドレス、または、ネットワークの IP アドレスを指定します。
パケット送信間隔	0
パケット送信回数	1

サービス監視パラメータ設定ガイド

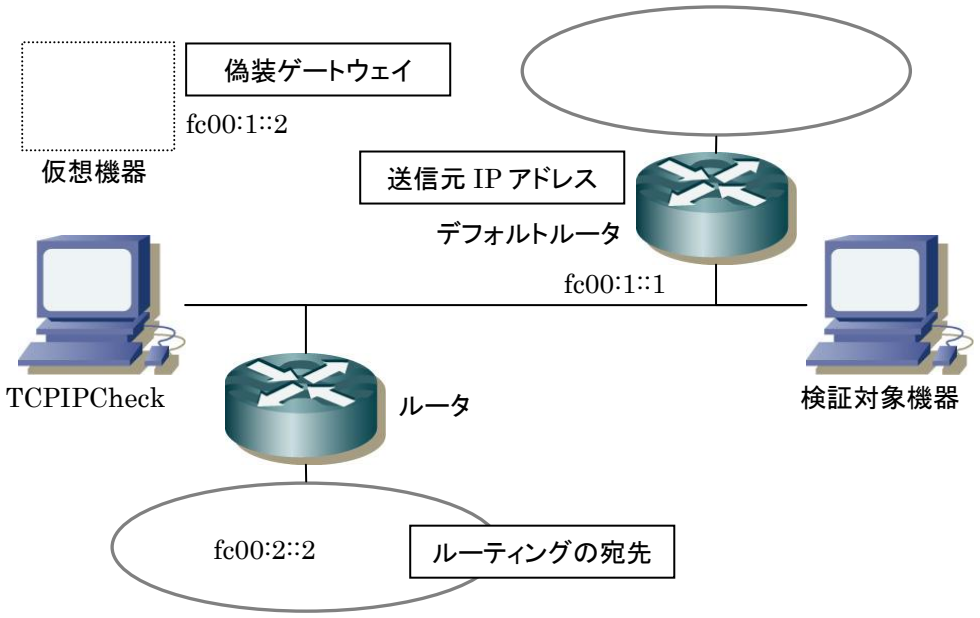
この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

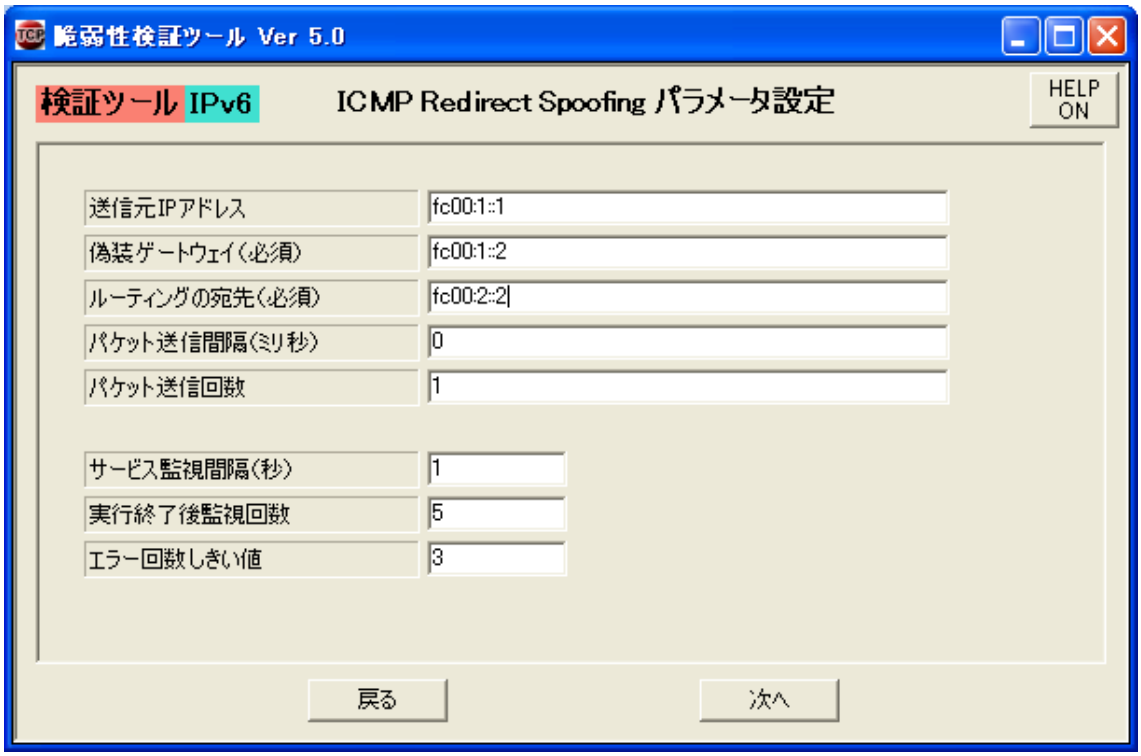
以下のような方法で、脆弱性有無の確認を行ってください。

- ルーティングの宛先で指定したホスト、または、ネットワークに対する通信ができなくなっていないか確認してください。
- 可能であれば、検証対象のルーティングテーブルを確認して、自分自身がゲートウェイとなっているエントリがないか確認してください。

[IPv6]



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP Redirect パケットを送信して、検証対象機器のルーティングテーブルを書き換え、送信先に攻撃者の IP アドレスを登録させることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が既に設定済みのゲートウェイ機器の IP アドレスを指定します。これは、検証対象が ICMP Redirect パケットを受け入れる確率を高くします。
偽装ゲートウェイ	検証対象機器と同一ネットワーク内の任意の IP アドレス。
ルーティングの宛先	通信を妨害させるホストの IP アドレス、または、ネットワークの IP アドレスを指定します。
パケット送信間隔	0
パケット送信回数	1

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

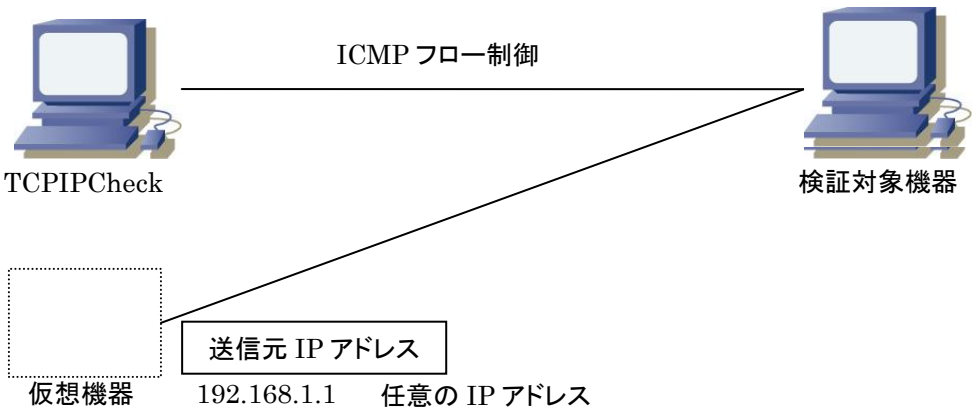
- ルーティングの宛先で指定したホスト、または、ネットワークに対する通信ができなくなっていないか確認してください。
- 可能であれば、検証対象のルーティングテーブルを確認して、自分自身がゲートウェイとなっているエントリがないか確認してください。

5)-16.ICMP Source Quench

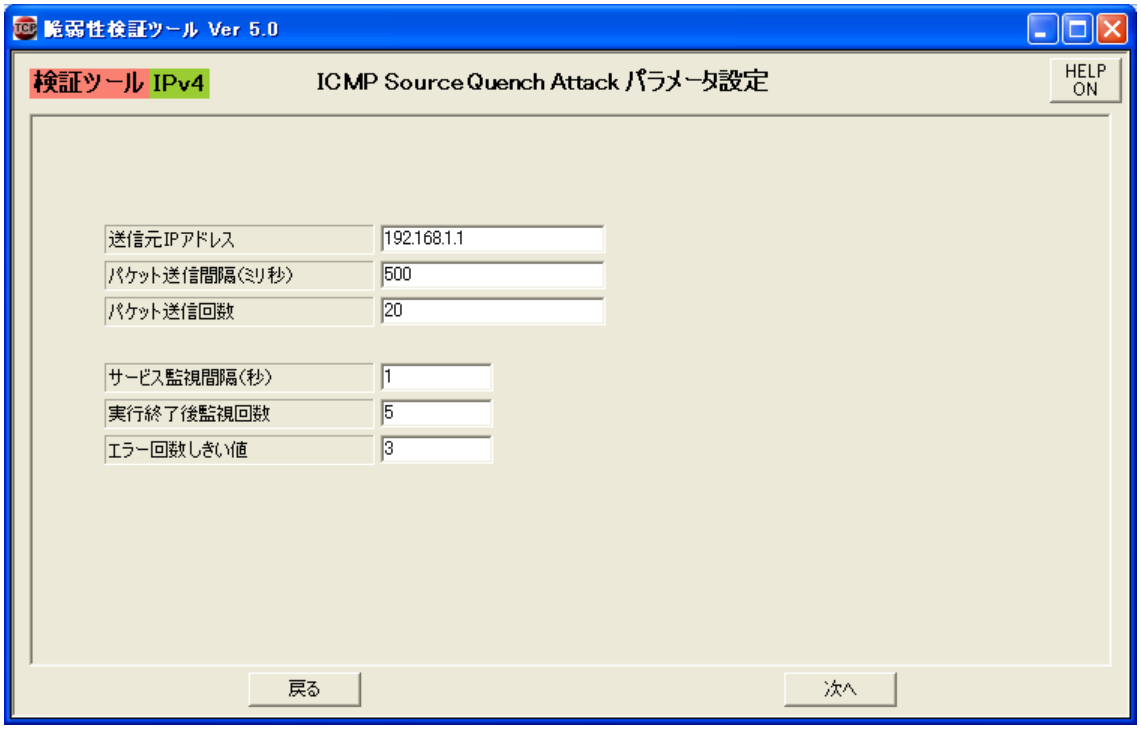
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：16) ICMP 始点制御メッセージによる通信遅延の問題

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP フロー制御(Source Quench)を送信し、検証対象機器のパケット送出速度を低下させることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
パケット送信間隔	500
パケット送信回数	20

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。

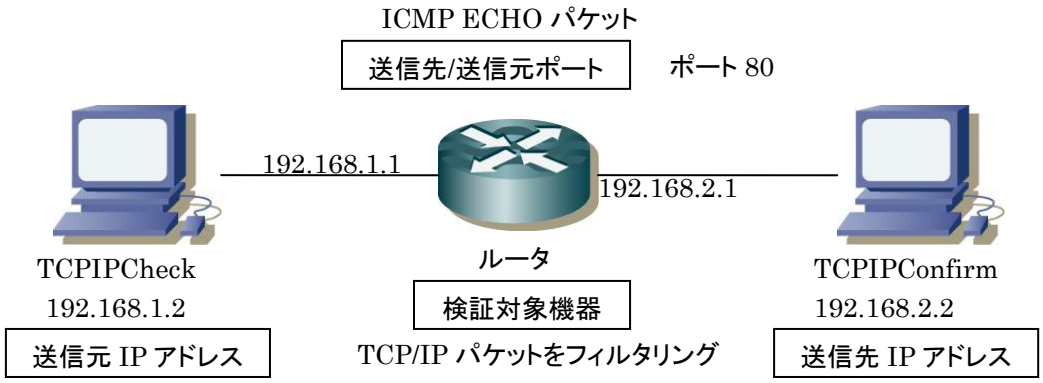
5)-17.ICMP トンネリング

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

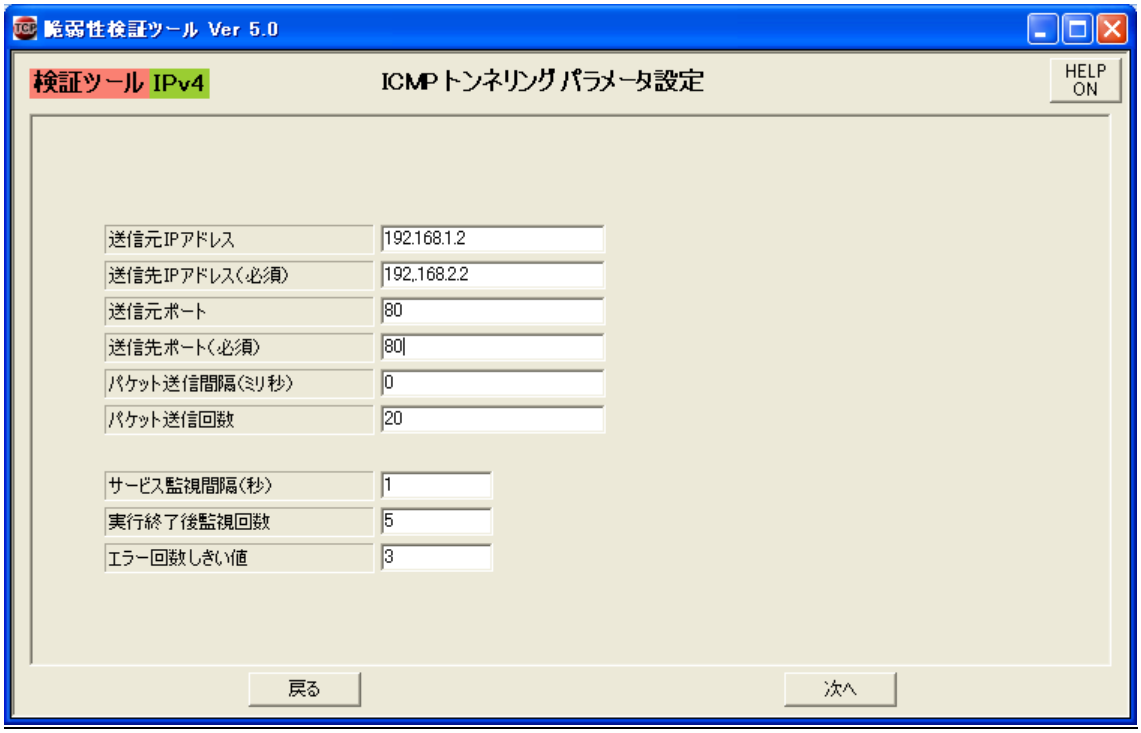
参照 : 17) ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題(ICMP トンネリング)

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

許可されていない TCP/IP の通信を ICMP でカプセル化する事によりフィルタリングを通過させる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先 IP アドレス	検証対象機器（ルータ）の先にある通信可能な機器の IP アドレスを指定してください。 TCPIPConfirm ツール(IPv4)を使用する時は、TCPIPConfirm ツール(IPv4)のパラメータ設定画面(P.77)に表示される"送信元 IP アドレス"を指定してください。
送信先ポート	検証対象の TCP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	0
パケット送信回数	20

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

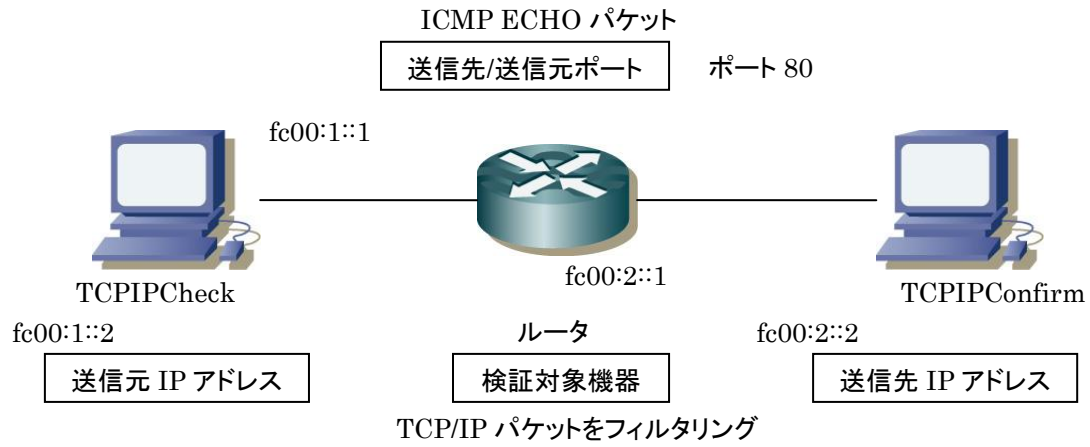
以下のような方法で、脆弱性有無の確認を行ってください。

- 送信先 IP アドレスで指定した機器で TCPIPConfirm ツール(IPv4)を起動し、パケットが到達していないか確認してください。

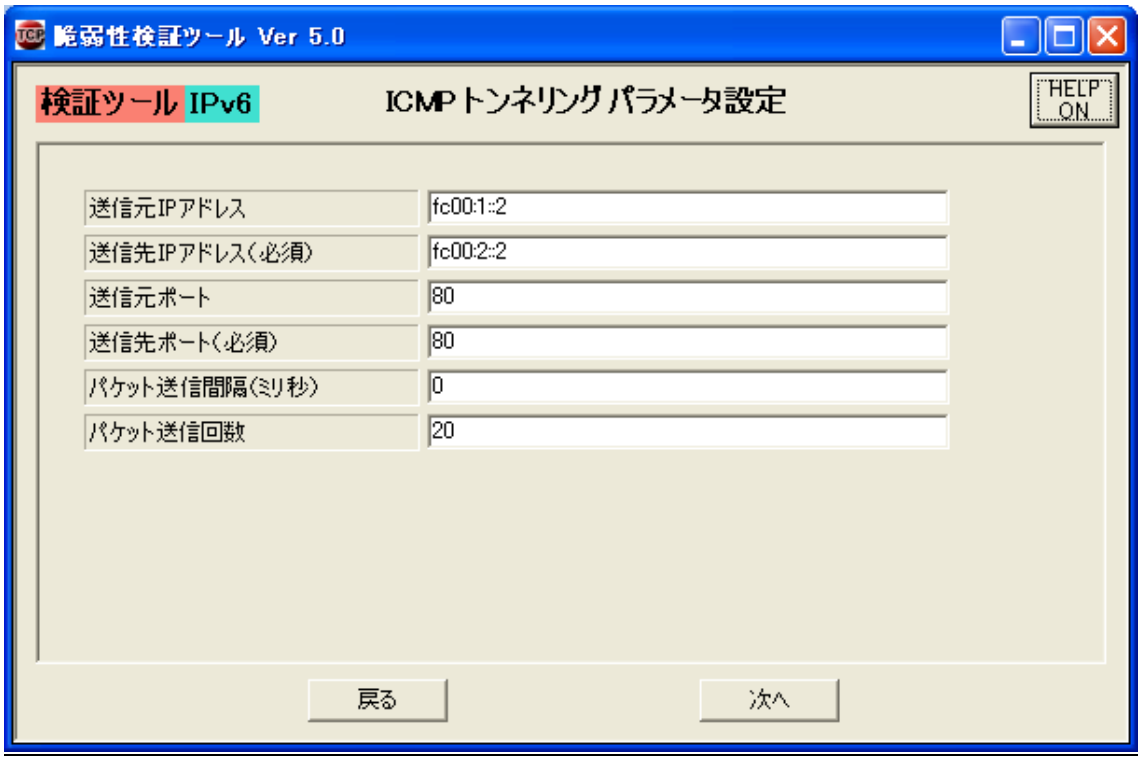
[IPv6]

[重要]この検証はユニークローカルユニキャストアドレスが正しく設定されていないネットワーク環境では正常に機能しません。

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

許可されていない TCP/IP の通信を ICMP でカプセル化する事によりフィルタリングを通過させる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先 IP アドレス	検証対象機器（ルータ）の先にある通信可能な機器の IP アドレスを指定してください。 TCPIPConfirm ツール(IPv6)を使用する時は、TCPIPConfirm ツール(IPv6)のパラメータ設定画面(P.78)に表示される"送信元 IP アドレス"を指定してください。
送信先ポート	検証対象の TCP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	0
パケット送信回数	20

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 送信先 IP アドレスで指定した機器で TCPIPConfirm ツール(IPv6)を起動し、パケットが到達していないか確認してください。

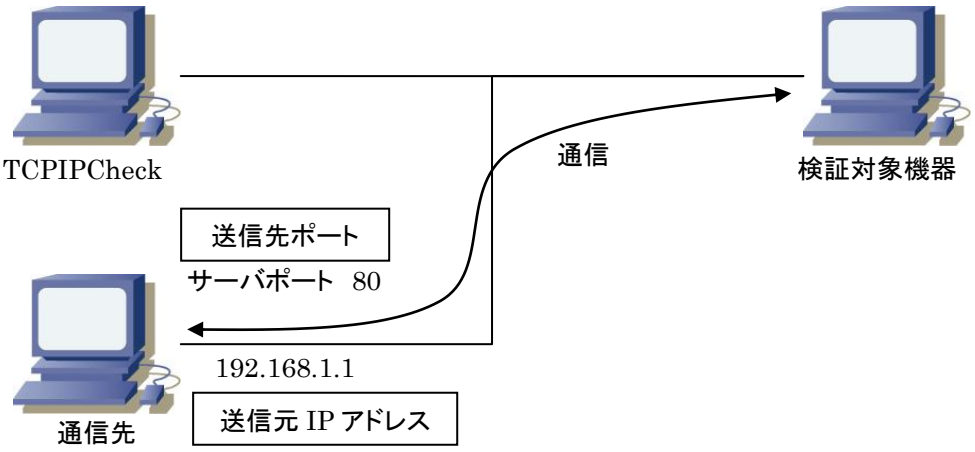
5)-18.ICMP blind connection reset

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

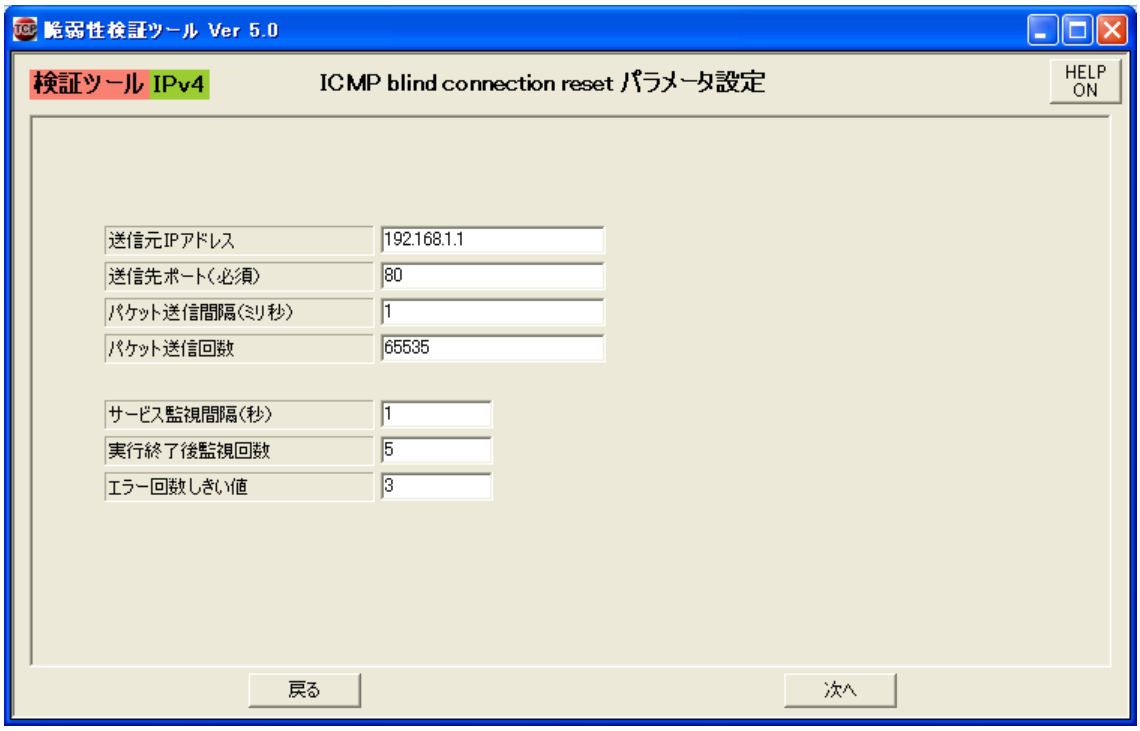
参照：18) ICMP エラーにより TCP 接続が切断される問題

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP エラーパケット（Destination Unreachable, Port Unreachable）を送信して、

検証対象機器の通信相手との接続を強制的に切断することが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が実際に通信を行っている機器の IP アドレスを指定してください。
送信先ポート	検証対象機器が実際に通信を行っている通信の、送信先ポート番号を指定してください。
パケット送信間隔	1
パケット送信回数	65,535

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

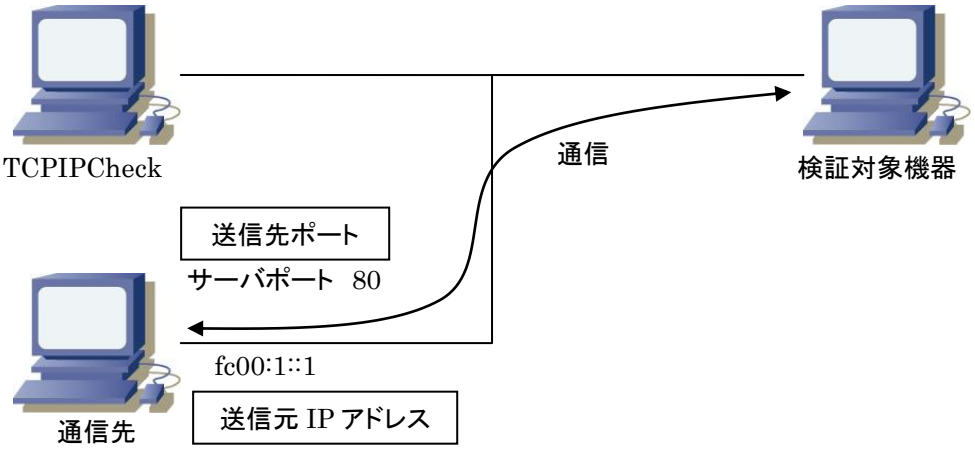
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

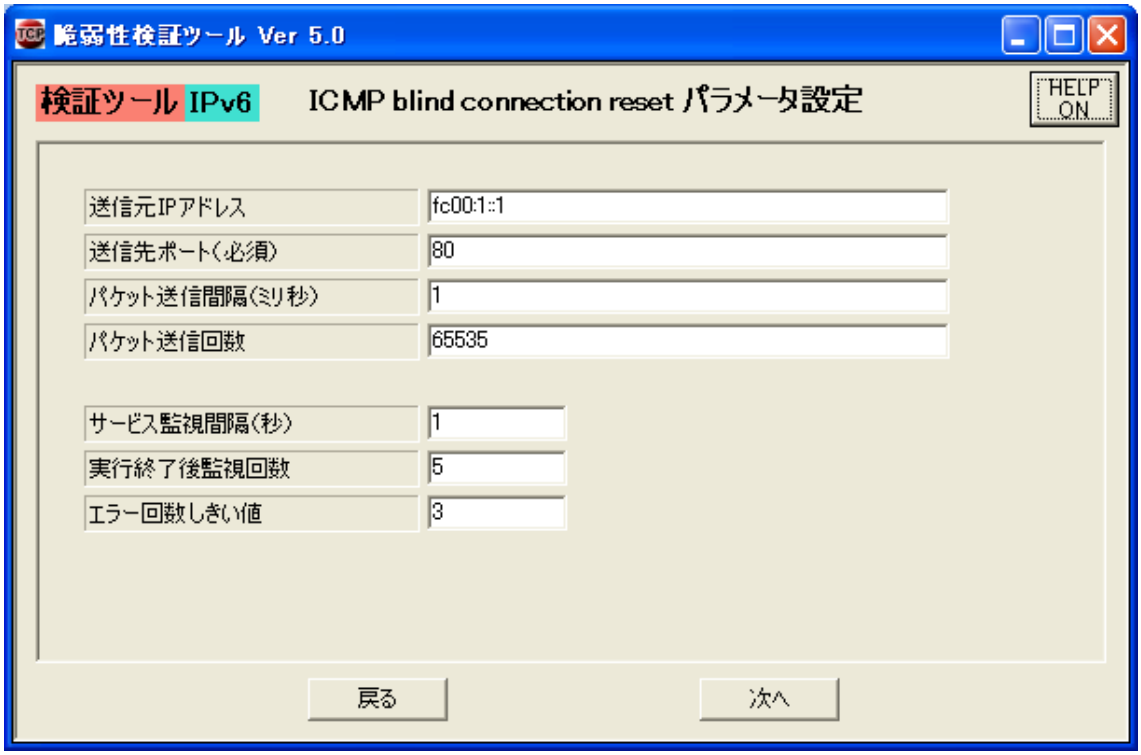
- ファイル転送等接続時間が長いオペレーションを行って、接続が切断されないか確認してください。
- この攻撃は、送信元ポート番号が 1 から 65535 までシーケンシャルに変化します。実際の接続で使用している送信元ポート番号と一致した時のみ、切断が行われます。65535 回送信すれば、送信元ポート番号が一巡します。

[IPv6]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

偽装した ICMP エラーパケット（communication with destination administratively prohibited）を送信して、検証対象機器の通信相手との接続を強制的に切断することが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	検証対象機器が実際に通信を行っている機器の IP アドレスを指定してください。
送信先ポート	検証対象機器が実際に通信を行っている通信の、送信先ポート番号を指定してください。
パケット送信間隔	1
パケット送信回数	65,535

サービス監視パラメータ設定ガイド

この脆弱性項目では、サービス監視は意味がありません。

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- ファイル転送等接続時間が長いオペレーションを行って、接続が切断されないか確認してください。

この攻撃は、送信元ポート番号が 1 から 65535 までシーケンシャルに変化します。実際の接続で使用している送信元ポート番号と一致した時のみ、切断が行われます。65535 回送信すれば、送信元ポート番号が一巡します

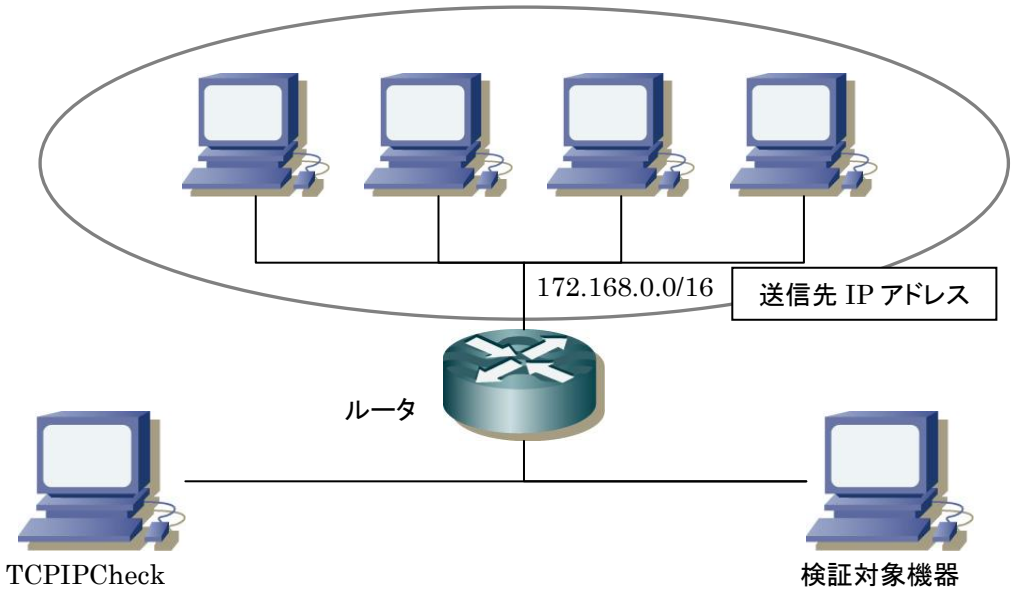
5)-19.Smurf Attack

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

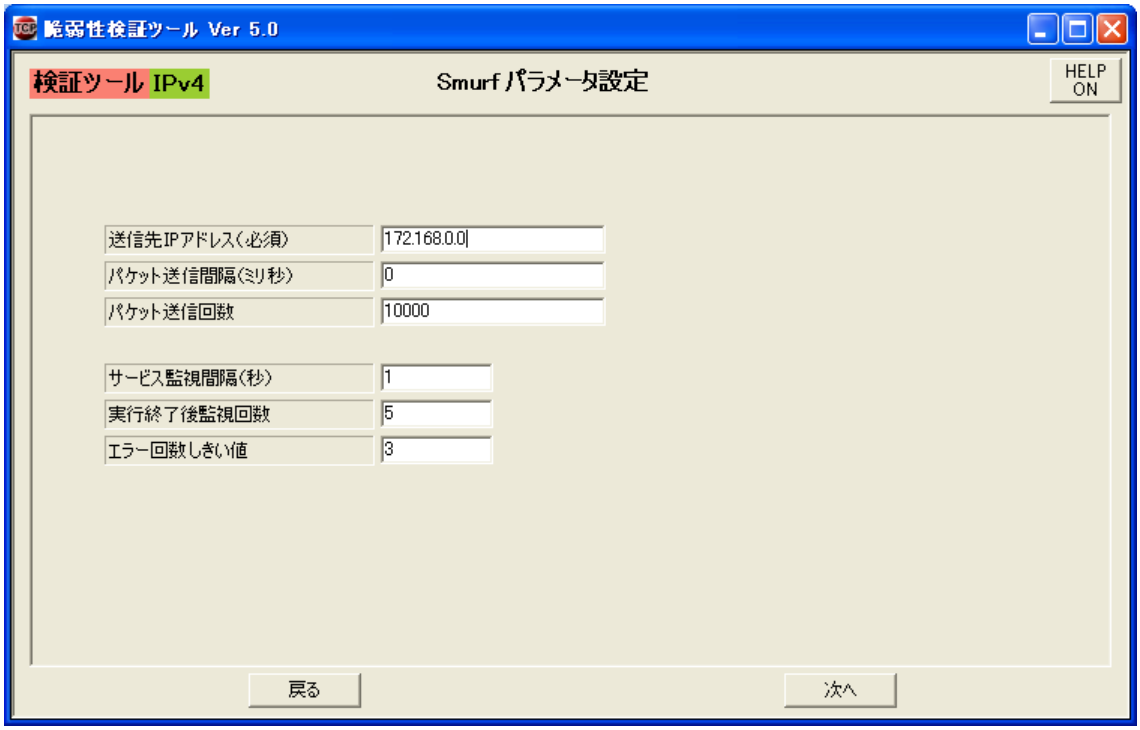
参照：19) ICMP Echo リクエストによる帯域枯渇の問題（Ping Flooding, Smurf Attack, Fraggle Attack）

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

送信元を検証対象機器の IP アドレスに偽装し、IP ブロードキャストアドレスを宛先とした ICMP Echo Request パケットを送信します。これにより、検証対象機器に大量の ICMP Echo Reply を送りつけ、サービスを妨害することが狙いです。この攻撃には、IP ブロードキャストに反応する複数の（多数の）ホストが必要になります。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信先 IP アドレス	複数のホストが存在する IP ブロードキャストアドレスを指定してください。
パケット送信間隔	0
パケット送信回数	10,000。

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

検証対象機器に対して

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

送信先 IP アドレスのホストに対して

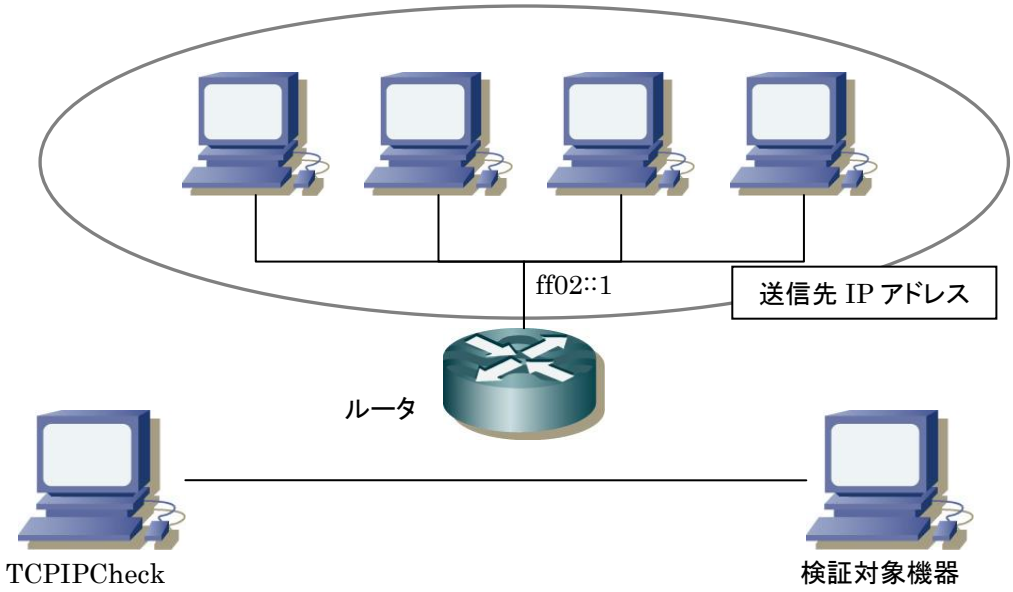
- IP ブロードキャスト宛のパケットに対して、反応するか否かを、パケットキャプチャを使用して確認してください。

ルータに対して

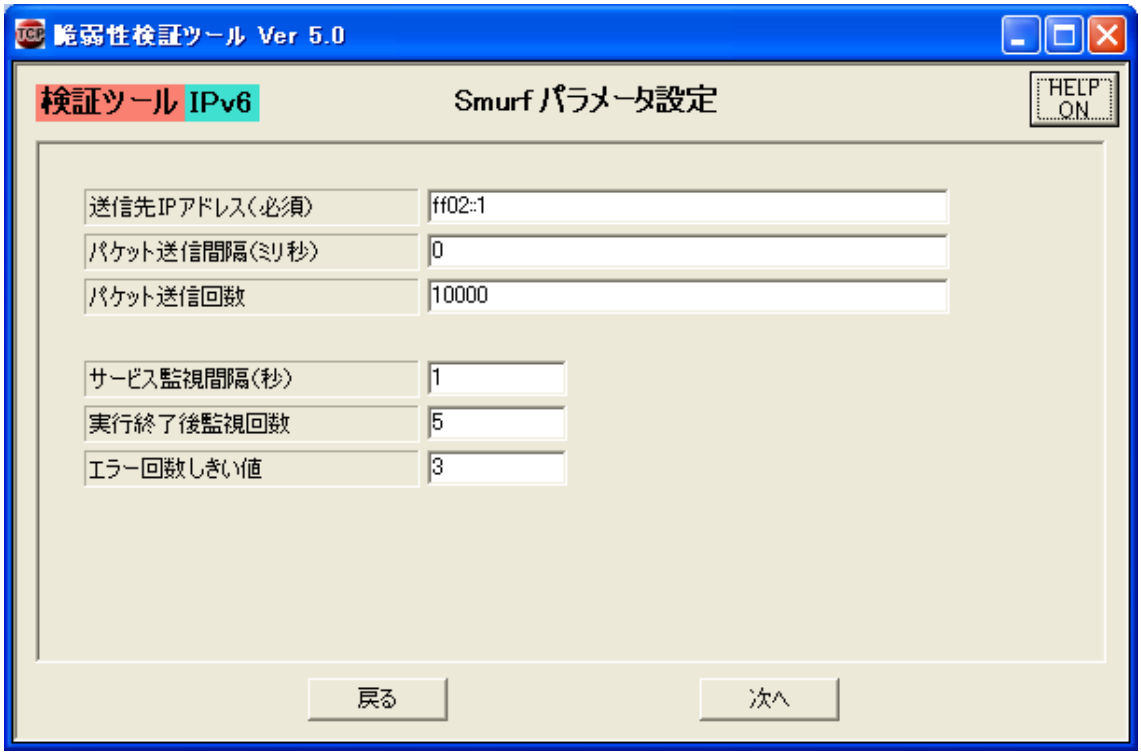
- IP ブロードキャスト宛のパケットを通過させるか否かを確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

送信元を検証対象機器の IP アドレスに偽装し、IP ブロードキャストアドレスを宛先とした ICMP Echo Request パケットを送信します。これにより、検証対象機器に大量の ICMP Echo Reply を送りつけ、サービスを妨害することが狙いです。この攻撃には、IP ブロードキャストに反応する複数の（多数の）ホストが必要になります。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信先 IP アドレス	複数のホストが存在する IP ブロードキャストアドレスを指定してください。
パケット送信間隔	0
パケット送信回数	10000

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

検証対象機器に対して

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

送信先 IP アドレスのホストに対して

- IP ブロードキャスト宛のパケットに対して、反応するか否かを、パケットキャプチャを使用して確認してください。

ルータに対して

- IP ブロードキャスト宛のパケットを通過させるか否かを確認してください。

5)-20.[未実装]ICMP タイムスタンプ要求/ネットマスク要求への応答による問題

未実装

5)-21.[未実装]IPv6 実装における Forwarding Information Base の更新に関する問題

未実装

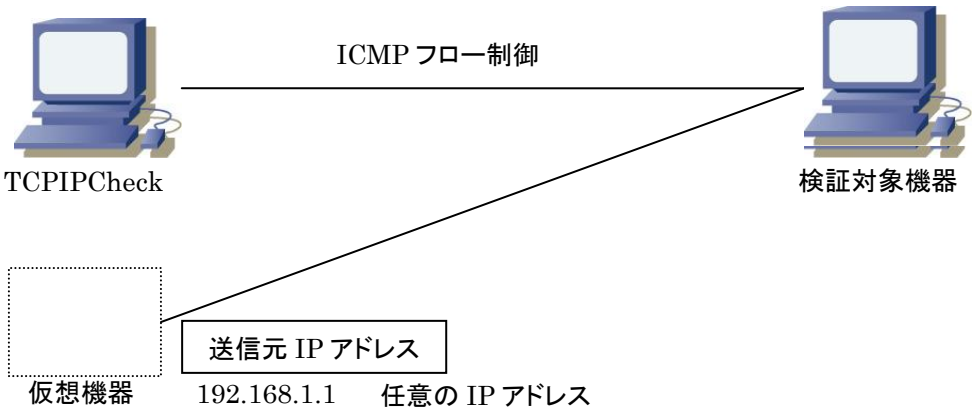
5)-22.Teardrop Attack

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

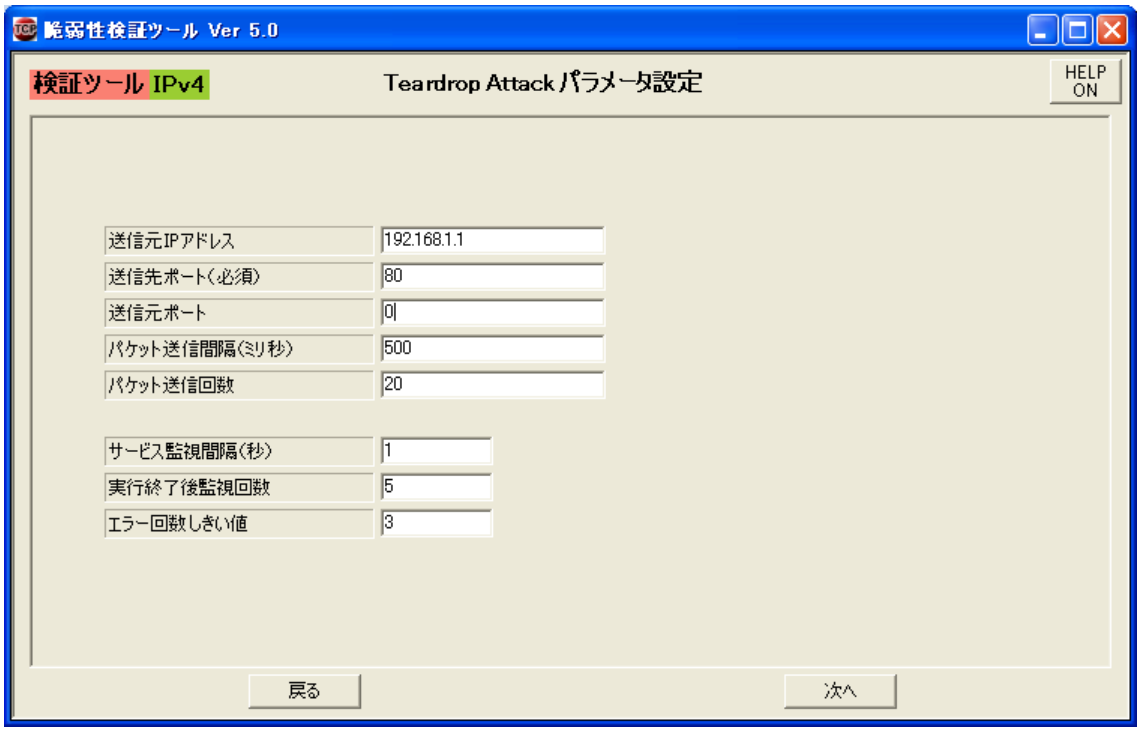
参照：22)フラグメントパケットの再構築時にシステムがクラッシュする問題（Teardrop Attack)

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

重複するフラグメントオフセット値を設定したパケットを送信し、検証対象機器においてパケットを正常に再構築できずにサービス不能状態にさせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先ポート	検証対象の OPEN 状態の UDP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	500 (ミリ秒)以上を指定してください。
パケット送信回数	1 から 20 くらいの間で十分です。

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

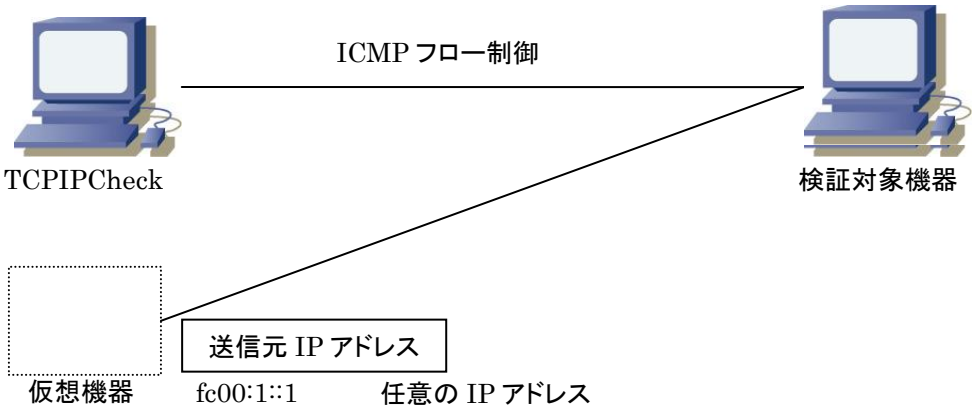
脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

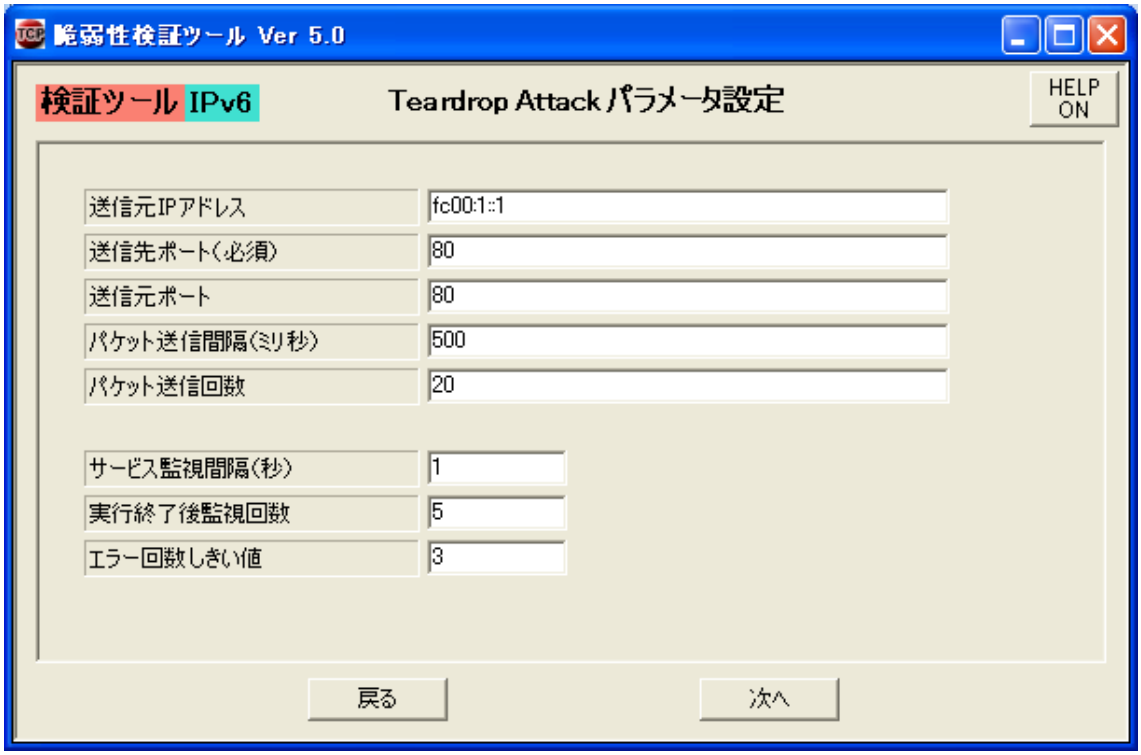
- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

[IPv6]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

重複するフラグメントオフセット値を設定したパケットを送信し、検証対象機器においてパケットを正常に再構築できずにサービス不能状態にさせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先ポート	検証対象の OPEN 状態の UDP ポート番号を指定してください。
送信元ポート	任意のポート番号を指定してください。
パケット送信間隔	500
パケット送信回数	20

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

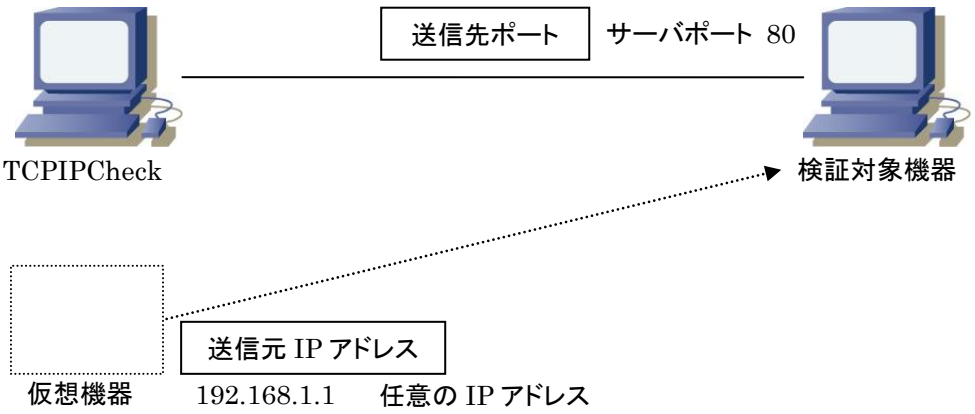
- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

5)-23.Rose Attack

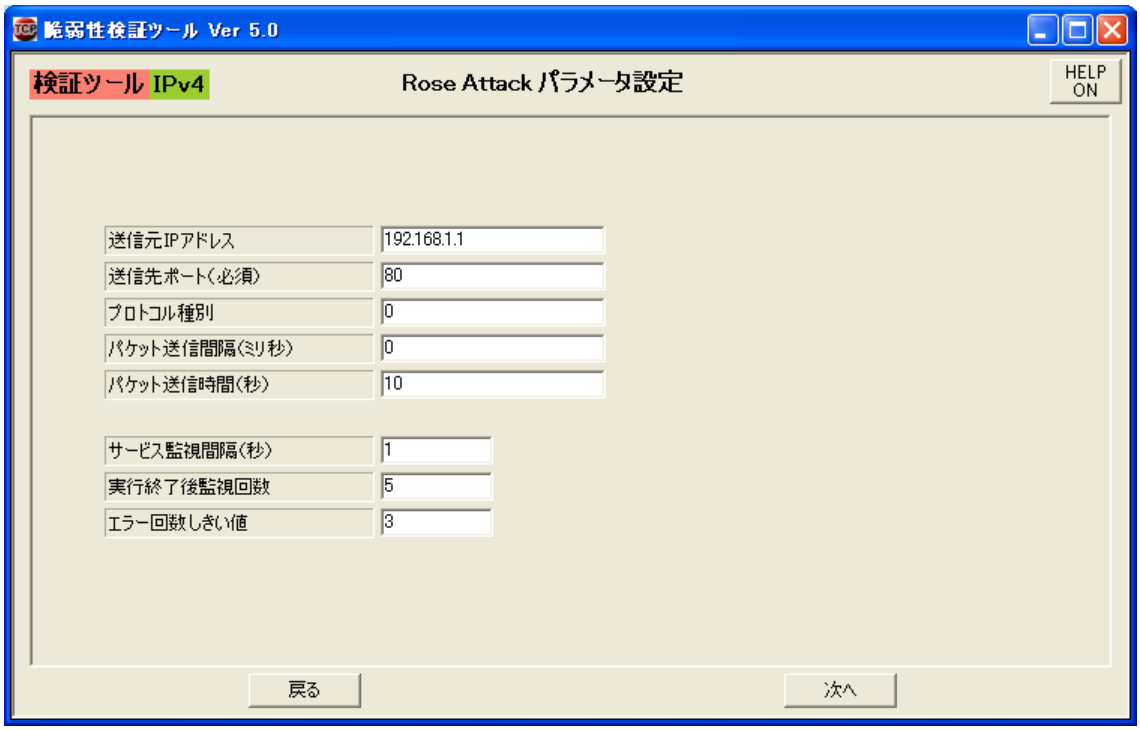
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：23) パケット再構築によりメモリ資源が枯渇される問題（Rose Attack）

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

すべてが揃わない IP フラグメントパケットを大量に送信することで、検証対象機器のメモリ資源を枯渇させ、機能不全にさせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
送信先ポート	次のプロトコル種別と合わせて、検証対象の OPEN 状態のポート番号を指定してください。
プロトコル種別	0 TCP 1 UDP
パケット送信間隔	0
パケット送信時間	検証対象機器の性能により異なるので、共通の推奨値はありません(最大指定可能値は 100 万秒です)。

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。
- この攻撃では、IP フラグメントパケットの処理が遅くなる、あるいは、できなくなる可能性があります。IP フラグメントが発生する大きなサイズの ping を受信できるか、あるいは、送信できるかを確認してください。

5)-24. [未実装]IP 経路制御オプションが検査されていない問題（IP Source Routing 攻撃）

未実装

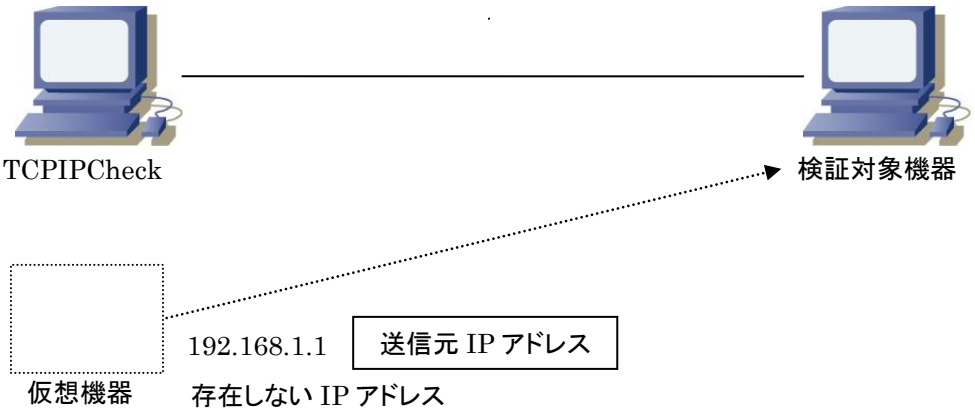
5)-25.IP ヘッダオプションのデータ長が 0 のパケットの問題

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

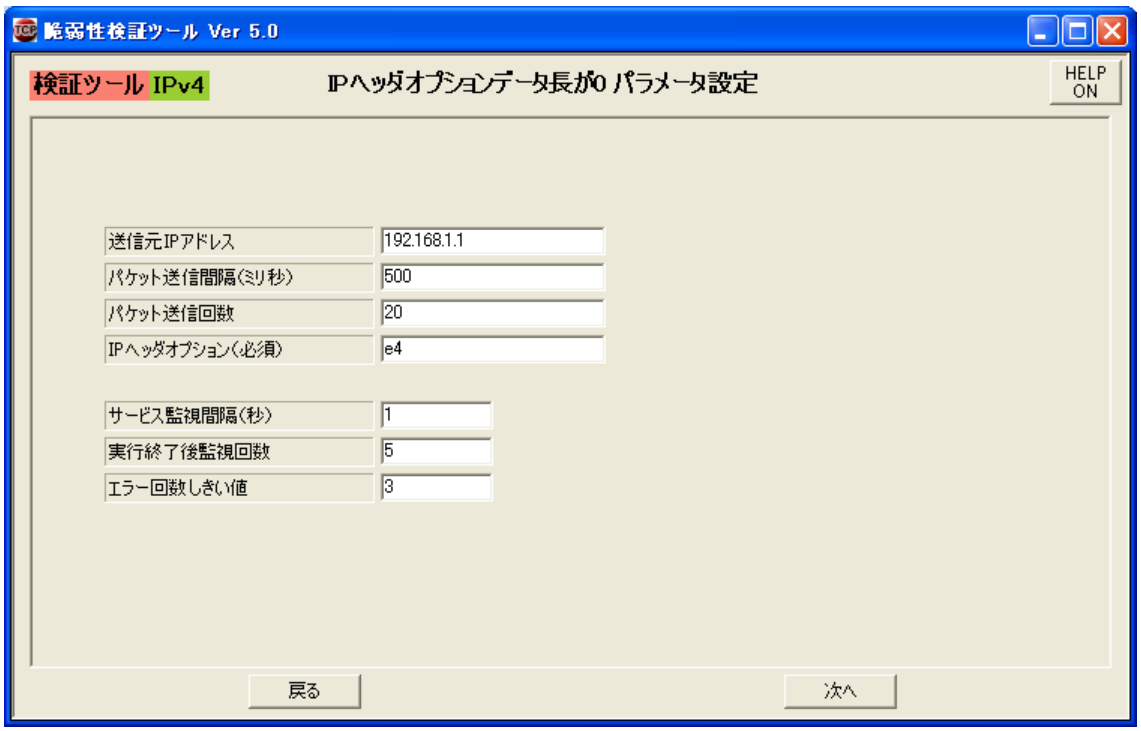
参照：25) IP ヘッダオプションのデータ長が 0 のパケットの問題

[IPv4]

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

IP ヘッダオプションのデータ長が 0 バイトのパケットを送信することで、検証対象機器をフリーズやクラッシュさせ、機能不全にさせる事が狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
パケット送信間隔	500
パケット送信回数	20
IP ヘッダオプション	e4(IP ヘッダオプションの先頭 1 バイトを 16 進数で指定します(英字は大文字、小文字とも入力可)。過去の事例で e4 の値が報告されています。)

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。
- ファイル転送等接続時間が長いオペレーションを行って、反応が遅くなっていないか確認してください。
- 可能であれば、検証対象の CPU の稼働率やメモリの使用状況を確認し、異常に大きな値になっていないか確認してください。

5)-26.[未実装]IP 経路制御機能(ソース・ルーティング機能)により、サービス不能状態に陥る問題

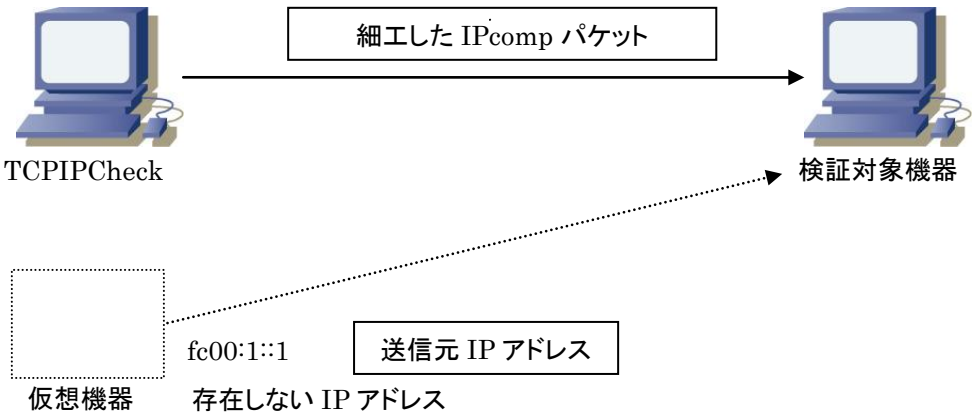
未実装

5)-27.IPv6 IPComp パケットの処理によりサービス不能状態に陥る問題

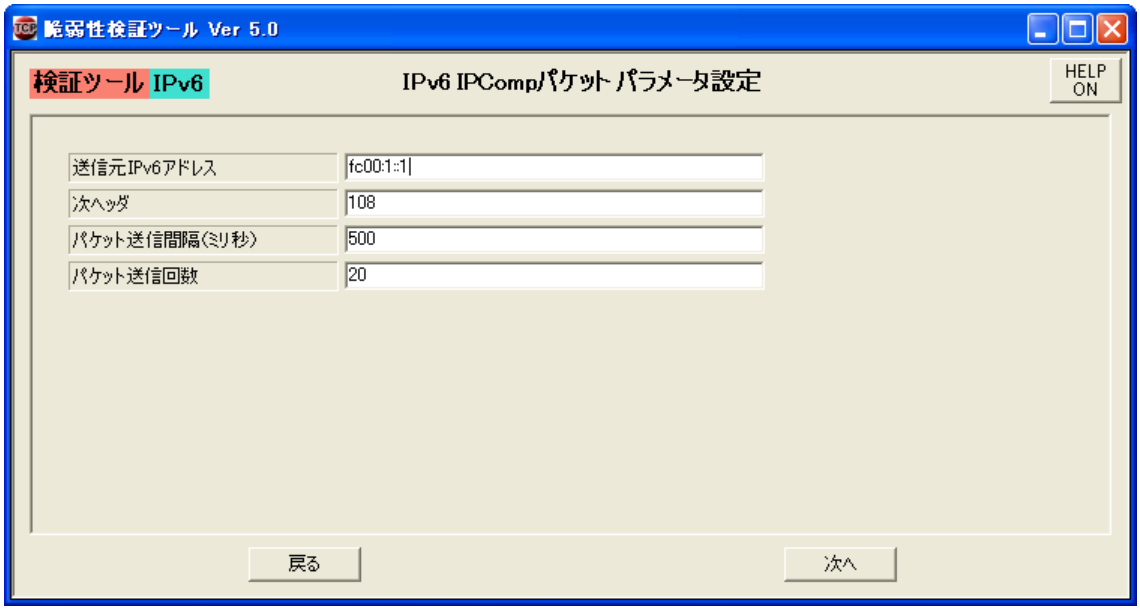
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：27) IPv6 IPComp パケットの処理によりサービス不能状態に陥る問題

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

本来はIPv6ヘッダに後続すべき拡張ヘッダを付加しない事で検証対象機器を機能不全にさせることが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	任意の IP アドレスを指定してください。
次ヘッダ	次ヘッダのヘッダ種別を 0～255 の範囲で指定してください。 未入力の時は 108(IPComp ヘッダ)を指定した事になります。
パケット送信間隔	500
パケット送信時間	20

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

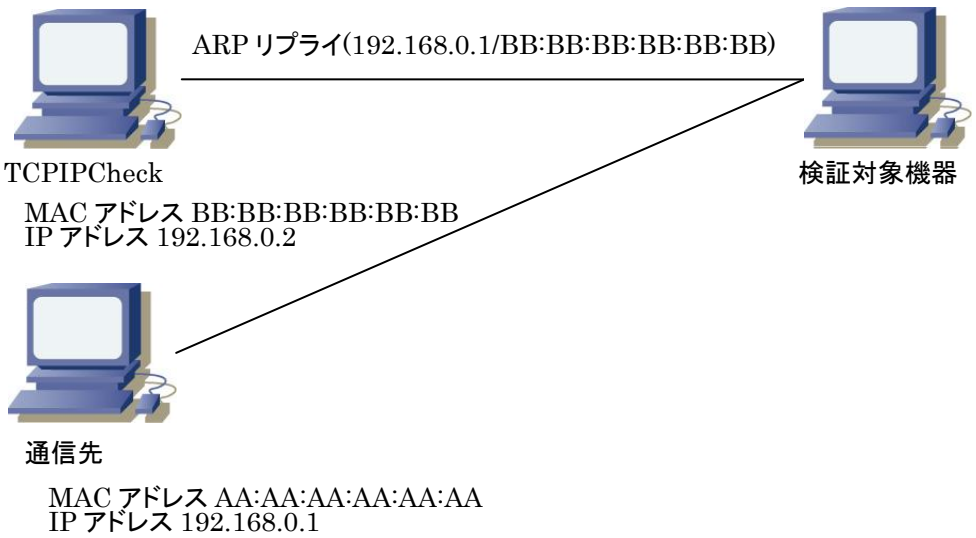
- 検証対象がハングアップや、再起動等の異常な状況にないか確認してください。
- 検証対象が通常行っているサービスにアクセスして、反応が遅くなっていないか確認してください。

5)-28.ARP Poisoning

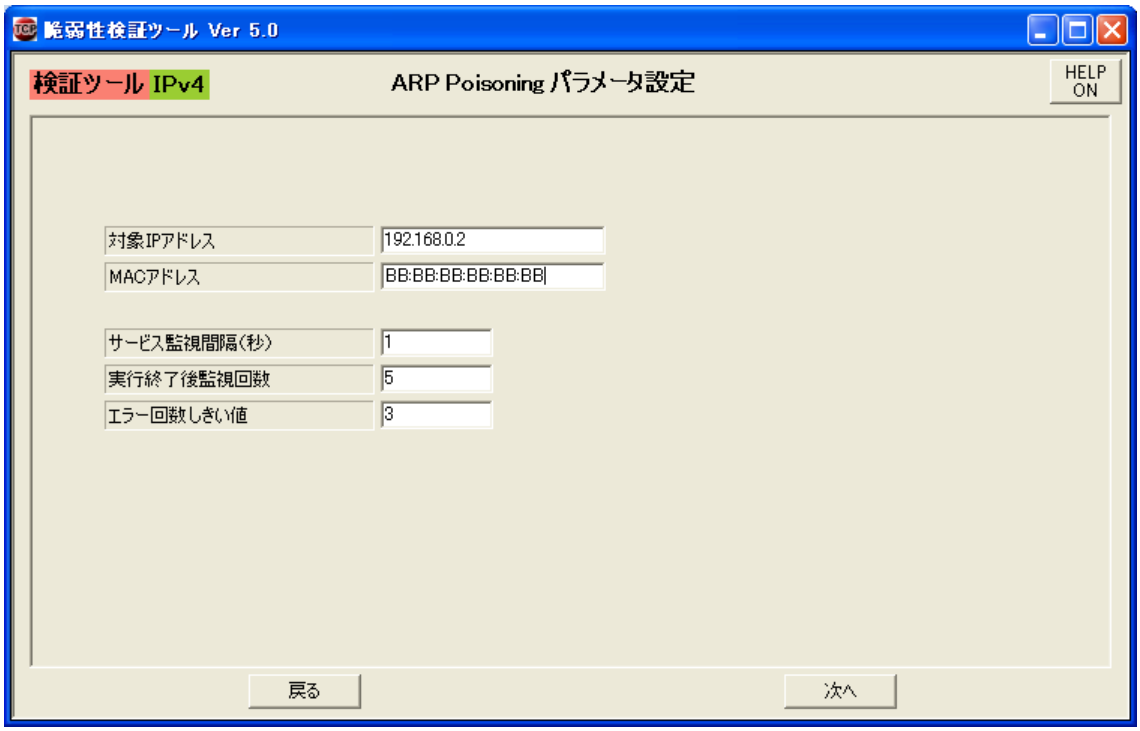
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：28)ARP テーブルが汚染される問題

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

不正な ARP リプライを送信し、検証対象機器の ARP テーブルを書き換え、通信をリダイレクトして盗聴したり、通信不能状態を発生させたりするのが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
対象 IP アドレス	ARP テーブル内の書換えをする IP アドレスを指定してください。
MAC アドレス	ARP テーブル内の上記 IP アドレスと対になる MAC アドレスを指定してください。

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- パラメータの対象 IP アドレスには、検証対象の ARP テーブルに既に存在する IP アドレス

を設定してください。

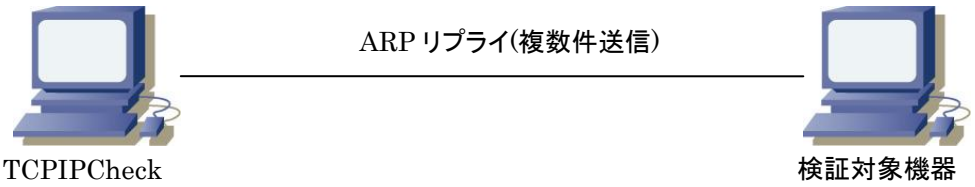
- 検証対象の ARP テーブルを確認し、指定した IP アドレス、MAC アドレスの値が登録されているか確認してください。
- 可能であれば検証対象に ARP テーブルに登録された IP アドレスを有する実機から Ping を実行し、通信ができるか確認してください。(前述のネットワーク構成の例で言うと”192.168.0.1”のホストから検証対象機器に対して Ping を実行してみてください。)

5)-29.ARP Flooding

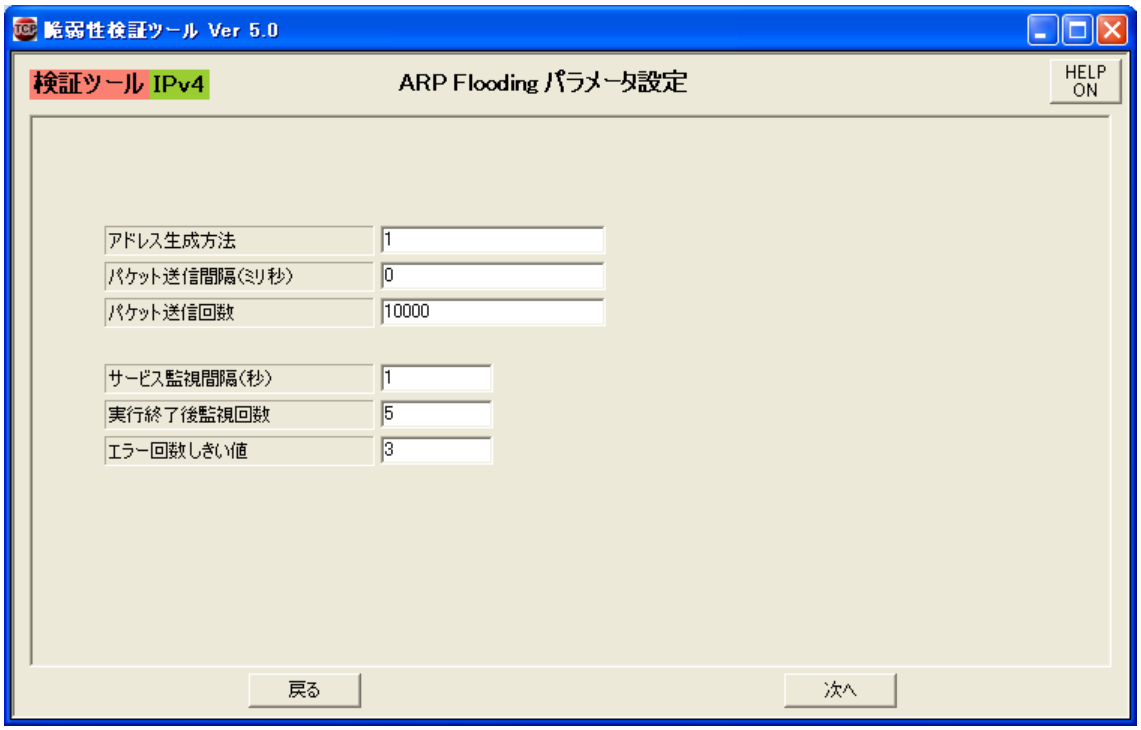
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：29)ARP テーブルが不正なエントリで埋め尽くされる問題

ネットワーク構成の例



パラメータ設定画面



攻撃パケットの概要

ランダムに生成した MAC アドレス、IP アドレスを連続的に送信し、検証対象機器の ARP テーブルを埋め尽くし、通信不能状態を発生させるのが狙いです。

脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
アドレス生成方法(*1)	検証目的により下記のいずれかを指定してください。 0 ランダム 1 ホストアドレスのみランダム
	“0”を選択した時は IP アドレス全桁についてランダムに生成します。 ”1”を選択した時は IP アドレス内のホストアドレス部のみランダムに生成し、ネットワークアドレス部については当該ネットワークのアドレスを使用します。例えば、IP アドレスが 192.168.0.1、ネットマスクが 255.255.255.0(クラス C)の時は 192.168.0.XXX の XXX の値のみランダムに生成します。この時、生成するアドレスは最大 255 個に限られる為、検証対象機器の ARP テーブルを埋め尽くすまでは至らない可能性があります。より多くの効果を期待する為にはクラス A またはクラス B のネットワーク環境で実行することをお勧めします。
パケット送信間隔	0
パケット送信回数	10,000

(*1)生成したアドレスが下記のものと一致した時は使用しない。

- 検索対象機器の IP アドレス
- TCPIPCheck を実行している機器の IP アドレス
- 当該ネットワークのデフォルトゲートウェイアドレス（TCPIPCheck を実行している機器の設定から求める）

サービス監視パラメータ設定ガイド

パラメータ名	推奨値
サービス監視間隔	1
実行終了後監視回数	5
エラー回数しきい値	3

脆弱性有無の確認方法

以下のような方法で、脆弱性有無の確認を行ってください。

- 検証対象の ARP テーブルを確認し、指定した IP アドレス、MAC アドレスの値が登録されているか確認してください。
- 可能であれば検証対象に ARP テーブルに登録された IP アドレスを有する実機から Ping を実行し、通信ができるか確認してください。

- 可能であれば検索対象機器から実存する機器に対して Ping などを使用し正常に通信できるか確認してください。

5)-30.[未実装]通常ではないパケットへの応答によって OS の種類が特定できる問題（TCP/IP Stack Fingerprinting）

未実装

◆ TCPIPConfirm（脆弱性確認ツール）編

1). はじめに

5)-31.このプログラムの目的

TCPIPConfirm は、TCPIPCheck（脆弱性検証ツール）が脆弱性の有無を確認する為に送信したパケットの到達を確認するためのプログラムです。

※ 本プログラム単体での使用は意味がありません。TCPIPCheck と併用してください。

※ 本プログラムは TCPIPCheck と同一のコンピュータにインストールすることはできません。

5)-32.機能概要

現在、インターネットプロトコル・バージョン 4 （以降 IPv4)、およびインターネットプロトコル・バージョン 6 （以降 IPv6）に関してそれぞれ 3 件の脆弱性項目の確認が可能です。これらの脆弱性はルータ等の中継機を対象としています。確認方法の概要としては、TCPIPCheck から検証対象となる中継機を経由し､本プログラムが稼動するコンピュータ宛にパケットを送信します。このパケットを本プログラムが受信した時、中継機に脆弱性有りと判断します。それぞれの脆弱性の詳細は､「TCP/IP に係る既知の脆弱性の調査報告書」の項目を参照してください。

1. Overlapping Fragment [IPv4] [IPv6]
   参照：5) データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題（Overlapping Fragment Attack)
2. Tiny Fragment [IPv4][IPv6]
   参照 : 6) 十分に小さい分割パケットがフィルタリングをすり抜ける問題 （Tiny Fragment Attack,Tiny Overlapping Fragment Attack）
3. ICMP トンネリング[IPv4][IPv6]
   参照：17) ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題 (ICMP トンネリング)

5)-33.動作環境

TCPIPConfirm は、以下のコンピュータ上で動作します。

Microsoft Windows XP Professional SP3 が動作する IBM AT 互換機
CD-ROM ドライブ、NIC を有する事

また、以下の環境を推奨します。

CPU	: Intel Pentium 4　2GHz 以上
ディスプレイ	: 画面解像度 1024 x 768 ピクセル以上
メモリ	: 1GBytes 以上

ハードディスク　　：1GBytes 以上の空き容量
NIC　　：Ethernet(100M 以上）のインターフェイスを有する事

2). インストール

以下の手順で、インストールを行ってください。

※ 前述の TCPIPCheck （脆弱性検証ツール） がインストールされている時、TCPIPConfirm をインストールすることはできません。TCPIPCheck をアンインストールしてから、以下の 2.の手順からインストールを行ってください。TCPIPCheck のアンインストール方法は、TCPIPCheck（脆弱性検証ツール）編 3).アンインストール）を参照してください。

※ インストールを行う時は、Administrators 権限を持つアカウントでインストールを行ってください。

1. 以下のサイトから、WinPcap (Windows Packet Capture Library) のインストーラをダウンロードし、インストールを行ってください。
   http://www.winpcap.org/install/default.htm
   WinPcap4.0.2 (2008 年 8 月 26 日最新) “WinPcap auto-installer (Driver +DLLs)”あるいは WinPcap4.1.1 (2010 年 7 月 02 日最新) “WinPcap auto-installer (Driver +DLLs)”
2. TCPIPConfirm インストール CD を CD ドライブにセットします。
3. スタートメニューから、[ファイル名を指定して実行]を選択し、”<CD ドライブ>:¥TCPIPConfirm¥Setup.Exe”をタイプし、[OK]ボタンをクリックします。
4. インストーラが起動し、TCPIPConfirm のインストールが開始されます。
5. この後の手順は、インストーラの指示に従って、インストールを行ってください。

3). アンインストール

以下の手順で、アンインストールを行ってください。

1. [スタートメニュー]-[コントロールパネル]-[プログラムの追加と削除]を選択してください。
2. [プログラムの追加と削除]ダイアログから、TCPIPConfirm の項目を選択し、[削除]ボタンをクリックしてください。TCPIPConfirm のアンインストールが開始されます。
3. 後は、インストーラの指示に従って、アンインストールを行ってください。
4. 同じく、[プログラムの追加と削除]ダイアログから、WinPcap を選択し、[変更と削除]ボタンをクリックしてください。
5. [WinPcap Uninstall]ダイアログの[Uninstall]ボタンをクリックしてください。
6. この後の手順は、インストーラの指示に従って、アンインストールを行ってください。

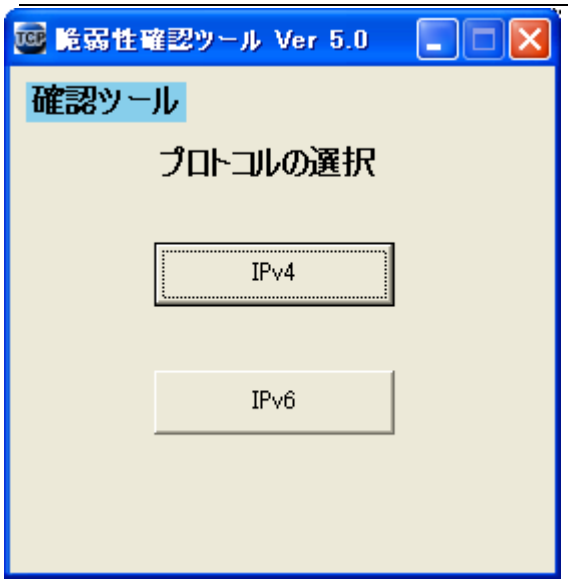
※ 4～6 は任意です。

4). 基本操作

5)-34.起動

スタートメニューから、[プログラム]-[IPA]-[TCPIPConfirm]を選択してください。プログラムが起動します。起動は Administrators 権限を持つユーザで行ってください。

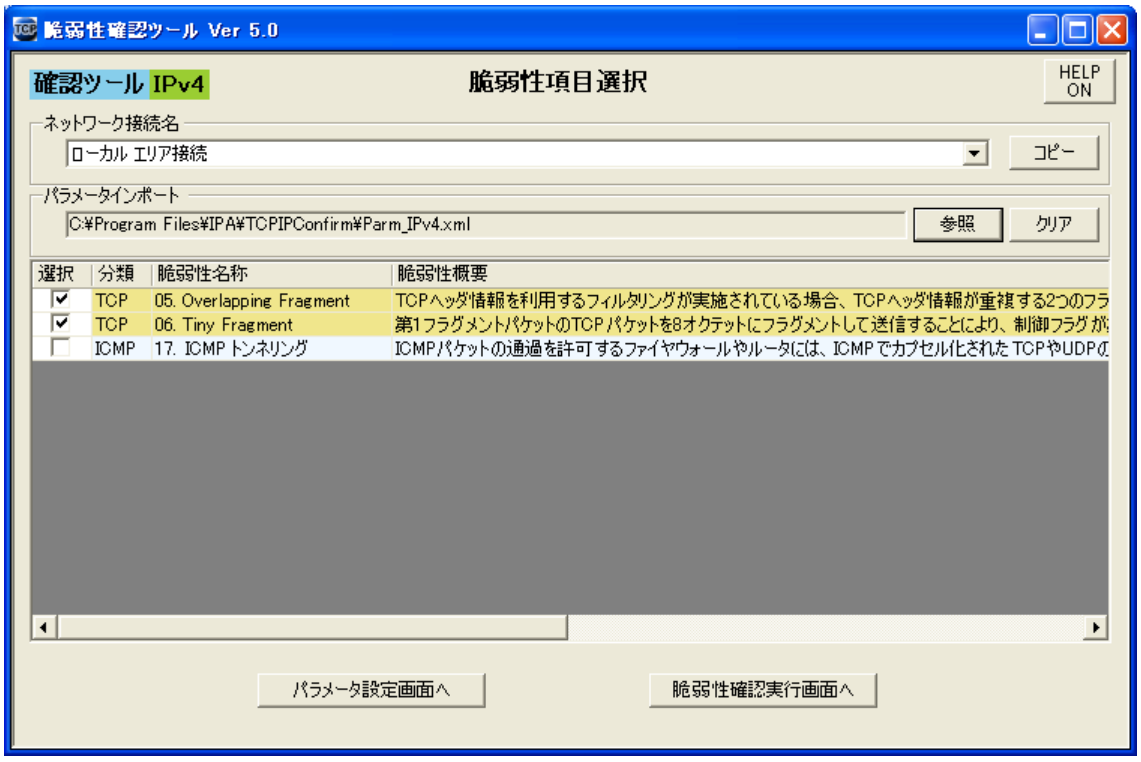
5)-35.プロトコルの選択



プロトコル選択画面では、以下の操作を行います。

1. 検証を行うプロトコルを選択します。
   "ネットワーク接続情報を取得できませんでした。"と表示される時、プロトコルが正しくインストールされているか確認してください。

5)-36.脆弱性項目の選択



4)-3.1. ネットワーク接続名の選択

検証を行う際に使用するネットワーク接続名を選択します。選択したネットワーク接続名を用いて、脆弱性パケットの受信が行われます。

1　ネットワーク接続名の選択方法

TCPIPConfirm をインストールしたコンピュータで、複数の有効なネットワーク接続名が存在する時は、[ネットワーク接続名]コンボボックスに複数のネットワーク接続名の名称がセットされています。確認に使用するネットワーク接続名を選択してください。

4)-3.2. [コピー]ボタン

クリップボードに選択しているネットワーク接続名をコピーします。コマンドライン起動を行う際に必要な設定ファイル[4)-13.4 参照]の作成を補助する機能です。利用方法は[4)-13.4]の、ConnectionName の欄を確認してください。

4)-3.3. 確認を行う脆弱性項目のチェック

確認を行う脆弱性項目の左の[選択]チェックボックスをチェックします。複数の項目をチェックすることが可能です。複数の項目をチェックした時、選択された脆弱性項目のパラメータを入力後、同時に確認を行います。

4)-3.4. パラメータのインポート

本ツールではパラメータファイルのインポートを行うことができます。パラメータのインポートを行うことにより、検証対象機を変更しても再び同じパラメータファイルをインポートすることにより、同じパラメータで検証を行うことができます。

1　パラメータのインポート方法

パラメータインポートの[参照]ボタンをクリックした時、[ファイルを開く]ダイアログが表示されるのでパラメータが入力されている xml ファイルを指定することにより、xml ファイルからパラメータがインポートされます。この時、パラメータのインポートが行われた脆弱性は[選択]チェックボックスにチェックがつきます。

2　インポートに使用するファイル

ファイルフォーマットに関しては、[4)-13.1]を参照してください。

3　[クリア]ボタン

パラメータのインポートを行った時、[クリア]ボタンが選択可能になります。[クリア]ボタンをクリックした時、全ての脆弱性の[選択]チェックボックスからチェックが外れ、入力されていたパラメータが全て空白になります。

4)-3.5. 画面遷移

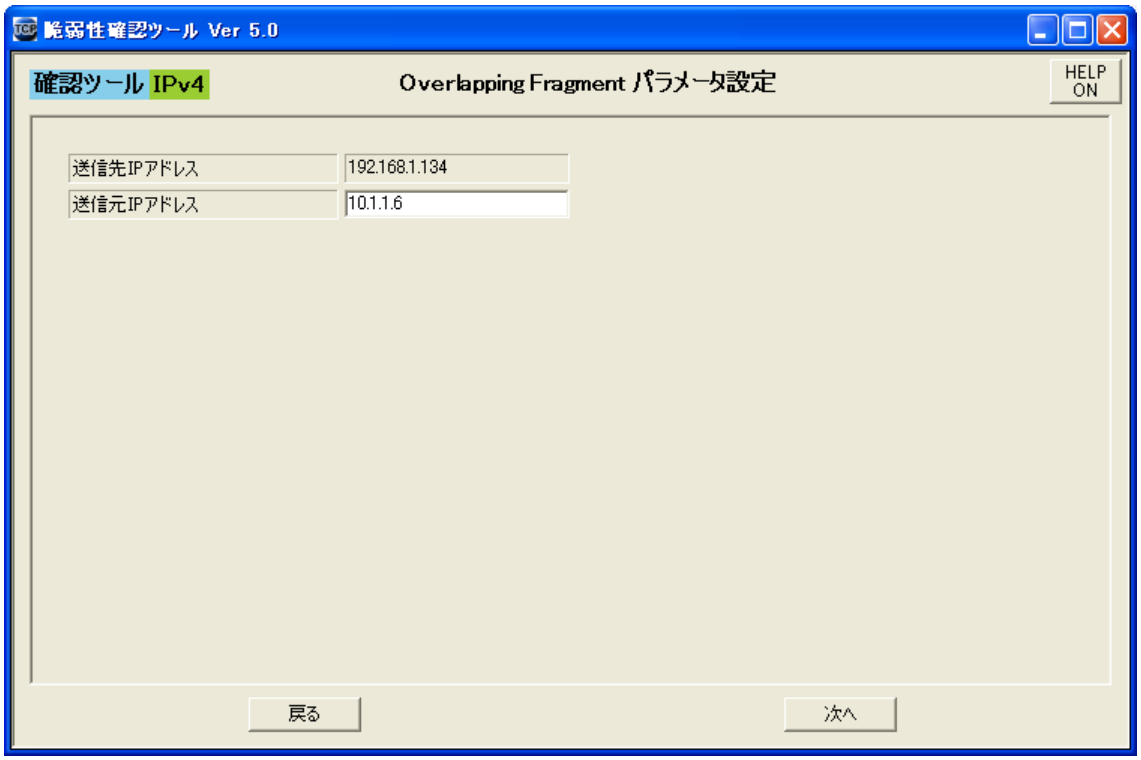
1　[パラメータ設定画面へ]ボタン

[パラメータ設定画面へ]ボタンをクリックした時、パラメータ設定画面へと遷移します。

2　[脆弱性実行画面へ]ボタン

パラメータのインポートを行った時、このボタンが選択可能になります。このボタンをクリックした時、[パラメータ設定画面へ]ボタンの処理に加え、選択した全ての脆弱性に対してパラメータのチェックが行われ、脆弱性実行画面へ遷移します。

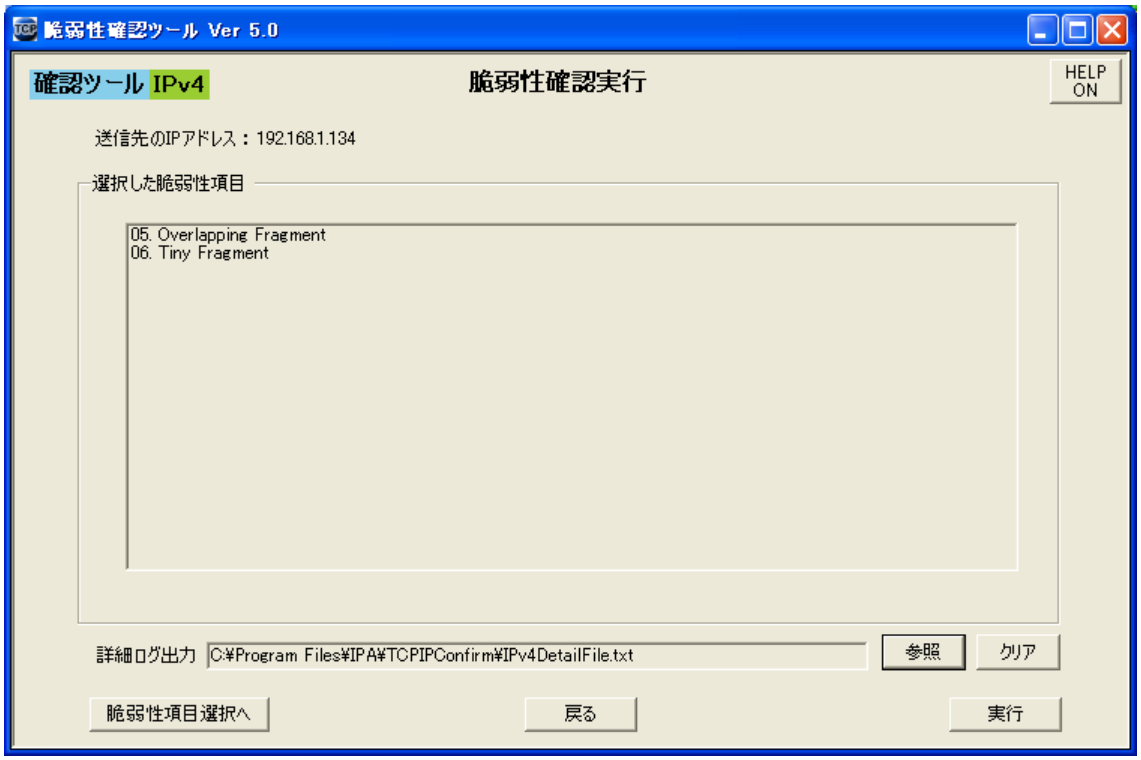
5)-37.パラメータの入力



パラメータ設定画面では、以下の操作を行います。

1. 脆弱性項目のパラメータを入力します。
   脆弱性項目を空欄にした時、その項目についてはパケットを確認する際の項目から除外されます。より厳密に確認を行う時は、空欄にしないでください。
2. パラメータ入力が完了しましたら、[次へ]ボタンをクリックしてください。
   次の脆弱性項目のパラメータ設定画面、または、脆弱性確認実行画面に移ります。

5)-38.確認の実行



脆弱性確認実行画面では、以下の操作を行います。

4)-5.1. 詳細ログの出力

本ツールでは、詳細ログの出力を行うことができます。詳細ログを出力することにより、各検証結果の比較を行うことができ、エラー発生時にその情報が出力されるようになります。指定を行わなかった時、詳細ログの出力は行われません。

1. 詳細ログの指定方法

   [参照]ボタンをクリックした時、[名前を付けて保存]ダイアログが開かれるので詳細ログの出力先を指定します。その場合、検証終了後に指定したファイルにテキストファイルでツールの詳細ログが出力されます。指定を行わなかった時、詳細ログは出力されません。また、詳細ログファイルの指定は出力先を直接指定することはできません。

2. 詳細ログの書式

   ファイルフォーマットに関しては、[4)-13.2]を参照してください。

3. [クリア]ボタン

   詳細ログを指定した時、[クリア]ボタンが選択できるようになる。[クリア]ボタンをクリックした時、詳細ログの指定がキャンセルされ、詳細ログは出力されません。

4)-5.2. [実行]ボタン

[実行]ボタンをクリックすると、確認を開始します。このとき詳細ログファイルの指定に既存のファイルを指定した時、ファイルに追記する旨を確認するメッセージボックスが表示されます。追記しても問題が無い時は[はい]を選択してください。[いいえ]を選択した時、脆弱性実行画面へ遷移します。

4)-5.3. 画面遷移

1. [戻る]ボタン

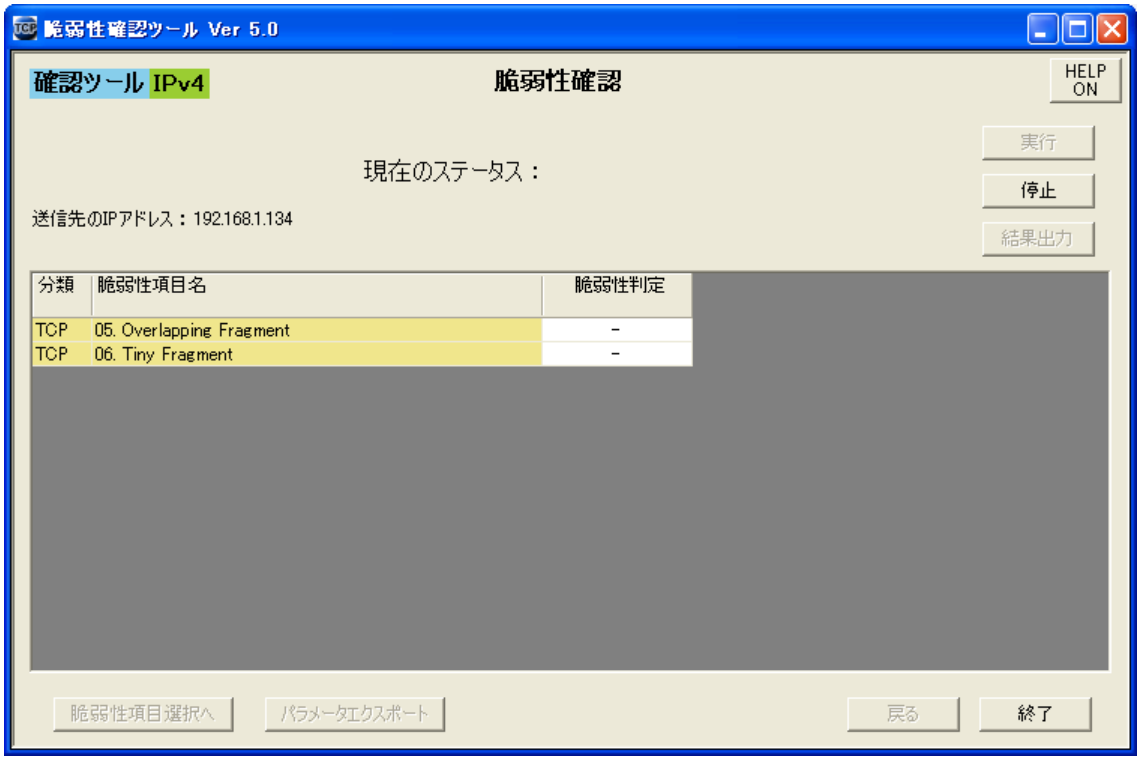
[戻る]ボタンをクリックすると、前の脆弱性項目のパラメータ設定画面に戻ります。

2. 「脆弱性項目選択へ]ボタン

「脆弱性項目選択へ]ボタンをクリックすると、脆弱性項目選択画面に戻ります。

5)-39.脆弱性有無の判定

以下は、確認実行中の画面の例です。



脆弱性確認画面では、以下の操作を行います。

1. [停止]ボタンをクリックすると確認を停止することができます。停止後、[実行]ボタンで確認を再開する事ができます。
2. [終了]ボタンをクリックすると処理を終了します。

脆弱性判定には、以下の表示があります。

表示内容	説明
―	まだパケットの到着が確認されていません。
有り	パケットの到着が確認されました。

TCPIPConfirm の脆弱性確認機能は、単純なパケットの到着結果を見ているに過ぎません。
実際の脆弱性の有無は、検証対象機器の状態を、検証者が確認する必要があります。

なお、脆弱性確認機能の終了には約 30 秒時間がかかります。

5)-40.脆弱性確認画面

4)-7.1 詳細ログの出力

本ツールでは詳細ログが指定されている場合、検証途中で出力されるログと、検証終了時にユーザが指定したファイルに出力される詳細ログの、二種類を出力します。

1. 検証途中で出力されるログ
   脆弱性の検証中、各実行プログラムは以下のファイルに詳細ログを出力していきます。

   <インストールディレクトリ>¥logs¥[脆弱性の configID].log

   これらのファイルには脆弱性毎の確認状況が記載されています。ツールが正常終了した時、出力されたファイルはフォルダ内から削除されます。
   確認ツールが異常終了した時、これらのファイルは削除されないため、どの処理を行っている時にツールが終了したのか、内容を閲覧することで確認することが可能です。

2. 検証終了時に出力される詳細ログ。
   詳細ログの指定を行っていた時、ユーザが指定したファイルに詳細ログの追記が行われます。

4)-7.2 検証結果ファイルの出力

本ツールでは、検証結果ファイルを出力することができます。検証結果の出力を行うことにより、検証結果の保存と各検証結果の比較も行えます。

1. 検証結果の出力方法
   [結果出力]ボタンをクリックした時、[名前を付けて保存]ダイアログが表示され検証結果ファイルの出力先を指定できます。ファイルを指定した時、新規ファイルである時は作成がそのまま行われます。既存のファイルを指定している時は、追記を行ってもよいか確認するメッセージボックスが表示されます。[はい]を選択すると、指定したファイルに検証結果が出力されます。[いいえ]を選択した時、検証結果は出力されません。

2. 検証結果ファイルの形式
   ファイルフォーマットに関しては、[4)-13.4]を参照してください。

4)-7.3 パラメータファイルの出力

本ツールでは、検証に使用したパラメータを xml ファイルでエクスポートすることができ

ます。エクスポートしたファイルは、パラメータのインポートで使用することができます。

1. パラメータファイルの作成
   [パラメータエクスポート]ボタンをクリックした時、[名前を付けて保存]ダイアログが表示されるのでファイルを指定すると、検証で設定したパラメータをファイルにエクスポートすることができます。新規のファイルを指定した時はそのまま出力が行われますが、既存のファイルを指定した時は上書きを行うか確認する旨を記載したメッセージボックスが表示され、[はい]をクリックすると指定したファイルに上書きされます。[いいえ]を選択すると、処理は終了します。

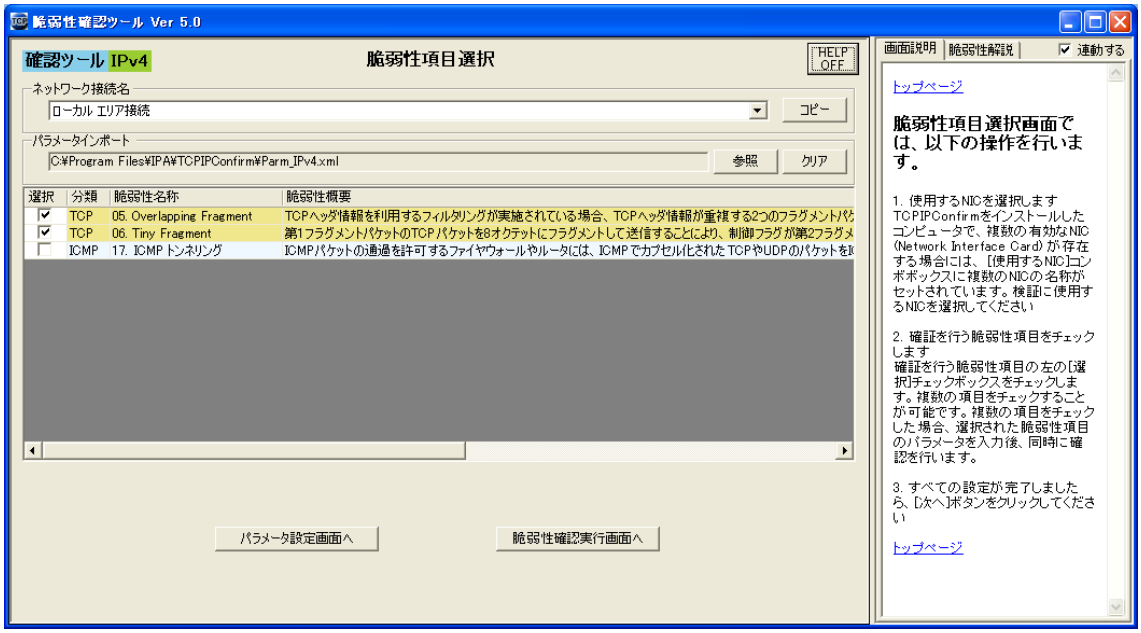
2. パラメータファイルの形式
   出力されるファイルの形式は、パラメータインポートでインポートしたファイルと同じ内容です。詳しくは[4)-13.1]を参照してください。

4)-7.4 画面遷移

1. [戻る]ボタン
   [戻る]ボタンをクリックした時、脆弱性実行画面へと遷移します。
2. [脆弱性項目選択へ]ボタン
   [脆弱性項目選択へ]ボタンをクリックした時、脆弱性選択画面へと遷移します。

5)-41.ヘルプ

各画面の[HELP ON]ボタンをクリックすると、ヘルプ画面を表示します。各画面の説明と、脆弱性解説の 2 種類のヘルプを参照できます。[連動する]チェックボックスをチェックすると、画面の遷移に応じてヘルプの表示内容も切り替わります。



5)-42.終了

脆弱性確認画面の[終了]ボタン、あるいは、各画面のタイトルバーの右端にある終了ボタンをクリックすると、プログラムが終了します。

5)-43.コマンドラインからの起動

本ツールでは、GUI 操作では対応することが難しい、ツールの自動化(バッチ処理)に対応するため、コマンドラインで起動することも可能です。コマンドラインで起動するためには、あらかじめ以下のファイルを用意しておく必要があります。

・設定ファイル
・パラメータファイル

4)-10.1 設定ファイル

コマンドラインで起動する際にパラメータとして指定するファイルです。コマンドライン起動時の処理は、設定ファイルに指定された内容で実行されます。書式は、[4)-13.4]を参照してください。

4)-10.2 検証で使用するパラメータファイルの作成方法

パラメータファイルは[4)-13.1]の形式のものを使用してください。指定したファイルに記載されている内容に則って検証が行われます

4)-10.3 検証の実行

1　コマンドプロンプト上で TCPIPConfirm.exe を起動し、パラメータとして設定ファイルを指定します。設定ファイルの内容の通り、検証が実行されます。以下に実行例を記載します。

4)-10.4 検証の終了

正常に検証が終了した場合、設定ファイルで指定した場所に検証結果ファイルが出力されます。詳細ログファイルは設定ファイルで指定されている時のみ出力されます。

4)-10.5 エラー出力

コマンドラインでの起動中、正常に検証が行えなかった時や処理が異常終了した時、エラーログファイルとイベントログにエラー情報が記載されます。

1. エラーログファイルの出力

エラーファイルの形式と出力内容は、検証ツールとの差異はありません。[4)-13.6]を参照してください。

2. イベントログへの出力

コマンドラインの起動中、エラーが起きた時はイベントログへの出力が行われます。
イベントログへの出力は以下の時に行われます。

・ツールの起動時
・ツールの終了時
・エラー発生時

イベントログの出力を確認したい時は[コントロールパネル]-[管理ツール]-[イベントビューア]-[アプリケーション]を確認してください。
このツールが出力したイベントログを参照したい時は、イベントソースで[脆弱性確認ツール Ver 5.0]で検索を行ってください。

4)-10.6 コマンドラインで起動する時の確認方法

コマンドライン起動時、以下のタイミングで動作確認を行う方法を記載します。

1. 起動の確認

イベントログに開始が書き込まれているか確認を行ってください。

2. 検証状況の確認

詳細ログの出力を行っている時、<インストールディレクトリ>¥log フォルダに、モジュールが出力したログが作成されるので、その内容をご確認ください。

3. 検証結果の確認

設定ファイルで指定したファイルに検証結果と詳細ログが出力されるので、内容をご確認ください。

5)-44.稼働ログファイルの削除

下記のディレクトリに稼動状況を記録した月別のログファイルを作成しています。これらのファイルは自動的には削除されませんので内容を確認し、不要なファイルは削除してください。内容の確認は[スタートメニュー]-[すべてのプログラム]-[アクセサリ]-[メモ帳]で行えます。（その他のテキストエディタでも内容の確認は可能です。）

- IPv4 の稼動ログファイルディレクトリ
  <インストールディレクトリ>¥log_IPv4
- IPv6 の稼動ログファイルディレクトリ
  <インストールディレクトリ>¥log_IPv6

5)-45. トラブルシューティング

以下のようなエラーメッセージが頻繁に表示される時は、TCPIPConfirm を再インストールする事をお勧めします。3).アンインストールを実行後、2).インストールを実行してください。エラーメッセージは、コマンドライン起動時はイベントログとエラーログ、画面で起動している時はメッセージボックスで表示されます。また、TCPIPConfirm を実行しようとした時にインストーラが作動してしまう時も、検証実行に必要なファイルが削除されている可能性がありますので、同様に再インストールする事をお勧めします。

主な、深刻なエラーメッセージは以下の通りです。

エラーメッセージ	エラー内容
NIC 情報を取得出来ませんでした。	NIC が正しく接続されていないか、ネットワーク接続が無効となっている時に出力されます。 ネットワークの設定を確認してください。
選択されたプロトコルに対して有効な NIC がありません。	
設定ファイルを読み込めませんでした。	設定ファイル（config_IPv4.xml または config_IPv6.xml）に不具合がある時に出力されます。 再インストールする事をお勧めします。
設定ファイルに脆弱性情報が正しく定義されていません。	
脆弱性検証モジュール（PMON_V4.exe または PMON_V6.exe）でエラーが発生しま	確認モジュールが他のプロセスから強制終了されてしまった時に出力されます。 もう一度、確認を実行してみてください。

した。エラーコード = 1、又は -1 詳細は、取扱説明書を確認してください。	
脆弱性検証モジュール （PMON_V4.exe または PMON_V6.exe）の実行に失敗しました。 詳細は、取扱説明書を確認してください。	検証モジュール exe ファイルが存在しない時に出力されます。 再インストールする事をお勧めします。
ディスクの容量が一杯になりました。	ファイルを出力しようとした先の空き容量が 1M 以下となっている時に出力されます。出力先のドライブに空き容量を作成してからファイルを出力し直してください。
コマンドライン起動設定ファイルが読み込めませんでした。	コマンドライン起動時のみ出力されます。 指定した設定ファイルが読み込めなかった時に表示されます。パラメータと、指定した設定ファイルの内容を確認してください。

5)-46.ファイル一覧

本ツールで用いられるファイルについて説明いたします。

4)-13.1 パラメータファイル

脆弱性項目の名称や各種パラメータ設定を記載するファイルです。

検証に使用するパラメータファイルは、パラメータのエクスポートで作成するか、以下のフォルダ内に存在するサンプルファイルを編集することで作成してください。パラメータファイルの作成は、パラメータエクスポートで行うことを推奨いたします。

IPv4 のパラメータファイル

<インストールディレクトリ>¥サンプル¥IPv4¥Parm_IPv4.xml

IPv6 のパラメータファイル

<インストールディレクトリ>¥サンプル¥IPv6¥Parm_IPv6.xml

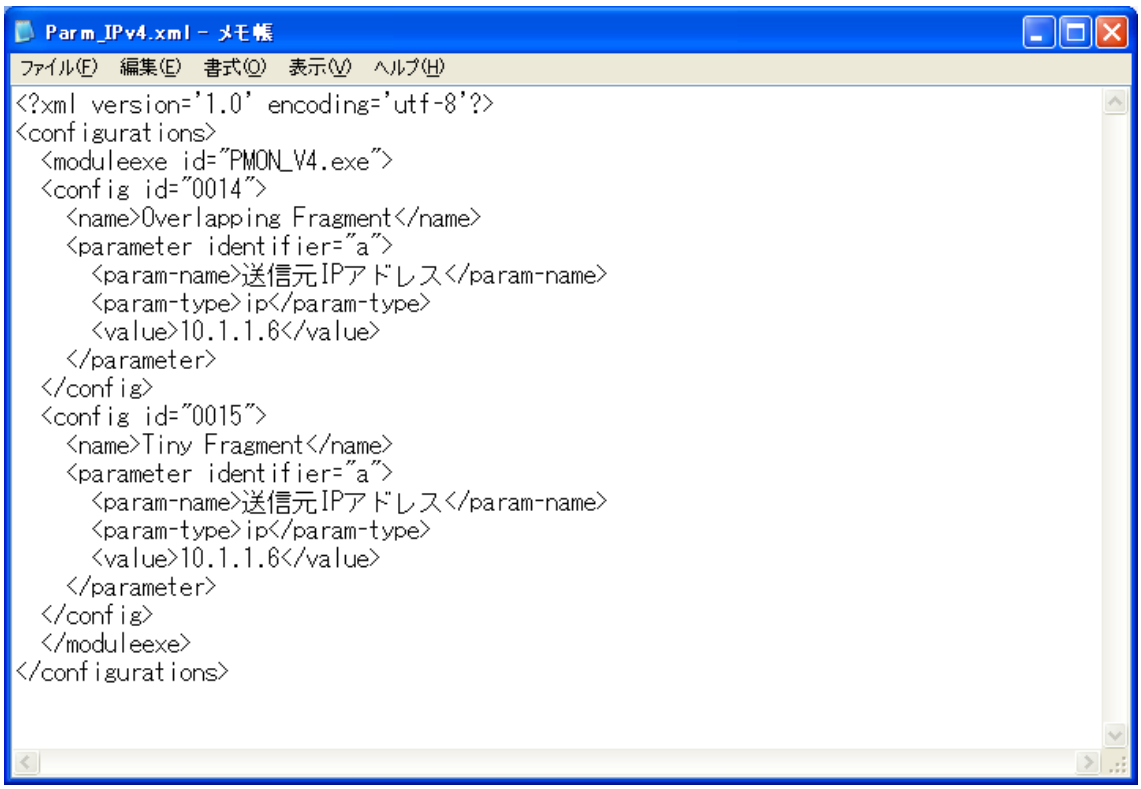
その場合、以下の内容で編集を行ってください。書式は xml 規格に準じます。

XML タグ	説明
moduleexe id	起動するモジュールの名称を入力します。

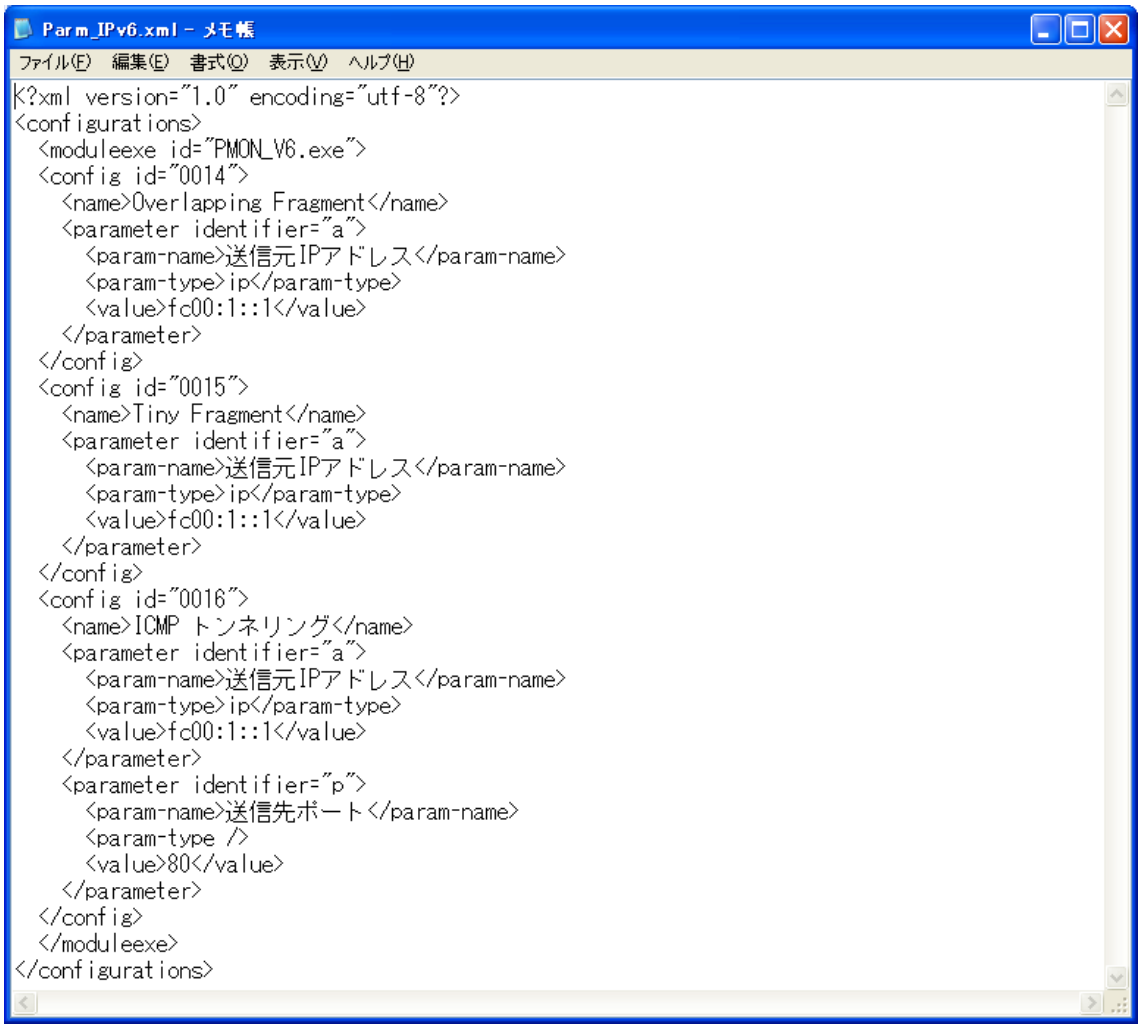
config id	脆弱性の config id を入力します。
name	脆弱性項目名を入力します。
parameter identifier	検証モジュールの個別パラメータごとに定義します。 属性 identifier にはパラメータ識別子を指定します。
param-name	パラメータ入力画面のラベルとして指定します。
param-type	IP アドレスの入力補正を行う項目の時に指定します。
value	入力値を指定します。

以下にパラメータファイルのサンプルを記載します。

IPv4



IPv6



4)-13.2 詳細ログファイル

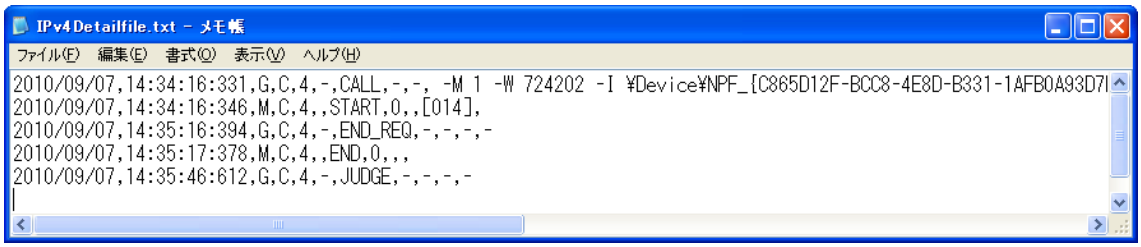
本ツールの稼働詳細ログファイルであり、ツールの起動/終了、各モジュールの起動・終了、脆弱性の有無判定時の情報や、エラー発生時の情報等を出力するファイルです。

詳細ログファイルは以下の内容で出力されます。形式はテキスト形式で、セパレータはカンマです。

日付,時刻,ツール識別子,ツール,プロトコル,モジュール ID,イベント,戻り値,脆弱性判定,パラメータ,付加情報

項目	説明
日付	ログが出力された日付、yy/mm/dd 形式で出力
時刻	ログが出力された時刻。HH:MM:SS:MMM 形式で出力
ツール識別子	ログを出力したのがどのツールなのかを表示する。以下の 2 パターンが存在する。 G：画面、 M：モジュール
ツール	検証ツールと確認ツールどちらで出力されたのか識別するためのパラメータ。以下の 2 パターンが存在する。 検証ツール：I 確認ツール：C
プロトコル	IPv4 と IPv6 どちらで出力されたのか識別するためのパラメータ。以下の 2 パターンが存在する。 4：IPv4 6：IPv6
モジュール ID	プログラム番号の数字 3 桁を表示する。
イベント	詳細ログが書き込まれたイベントを表示する。確認ツールでは以下の 6 パターンが存在する。 CALL：画面側がモジュールを呼び出したイベント START：モジュールが起動したイベント FIND：脆弱性を見つけたイベント END_REQ：モジュールへの終了指示を送ったイベント END：モジュールが終了したイベント JUDGE：画面側が脆弱性を判断したイベント
戻り値	モジュールの終了コードを表示する。 －：パケットの到着が確認できなかった。 有り：パケットの到着が確認された。
脆弱性判定	脆弱性判定の結果を表示する。
パラメータ	モジュール起動時のパラメータを表示する
付加情報	エラー及び脆弱性判定理由を表示する。

以下に詳細ログファイルのサンプルを記載します。



4)-13.3 検証結果出力ファイル

脆弱性検証後の検証結果を出力するファイルです。

検証結果ファイルは以下の内容で出力されます。ファイルの形式は CSV 形式です。セパレータはカンマです。

日付,時刻,送信先 IP アドレス,脆弱性項目名,脆弱性判定

項目	説明
日付	脆弱性検証/確認が終了した日付。YYYY/MM/DD 形式で出力
時刻	脆弱性検証/確認が終了した時刻。 HH:MM:SS 形式で出力
送信先 IP アドレス	検証対象機器の IP アドレス
脆弱性項目名	対象脆弱性項目の番号と名称
脆弱性判定	脆弱性判定の結果が表示されます。以下の２パターンが存在します 有り：パケットの到着が確認されました。 －：パケットの到着が確認されていません。

以下に結果出力ファイルのサンプルを記載します。

4)-13.4 設定ファイル

設定ファイルは、コマンドラインでツールを稼働させるときに必要なパラメータが記載されているファイルです。形式は ini ファイルです。

設定ファイルの作成を行う時、下記表を参考に新規に作成を行うか、以下のフォルダ内に存在するサンプルファイルを編集することで作成を行ってください。設定ファイルの作成はサンプルファイルをコピーし、編集して作成することを推奨します。

IPv4

<インストールディレクトリ>¥サンプル¥IPv4¥IPv4.ini

IPv6

<インストールディレクトリ>¥サンプル¥IPv6¥IPv6.ini

パラメータ名	説明	必須
[CommandLine]	セクション。[CommandLine]で固定。	●
Protocol	IPv4,で検証する時は IPv4、 IPv6 で検証する時は IPv6 を記入します。	●
Timer	コマンドラインでは、確認ツールを終了させる方法が無いため、動作し続ける時間を設定します。単位は分です。未入力の時は 10 分となります。指定できる数は 10000 分までです。入力する値としては、検証ツールが稼働する時間と同じ値を入力してください。	○
ConnectionName	使用するネットワーク接続名を指定します。	●
SetParam	検証に使用するパラメータファイル名を記入します。	●
ResultFile	検証結果の出力先となるファイル名を記入します。	●

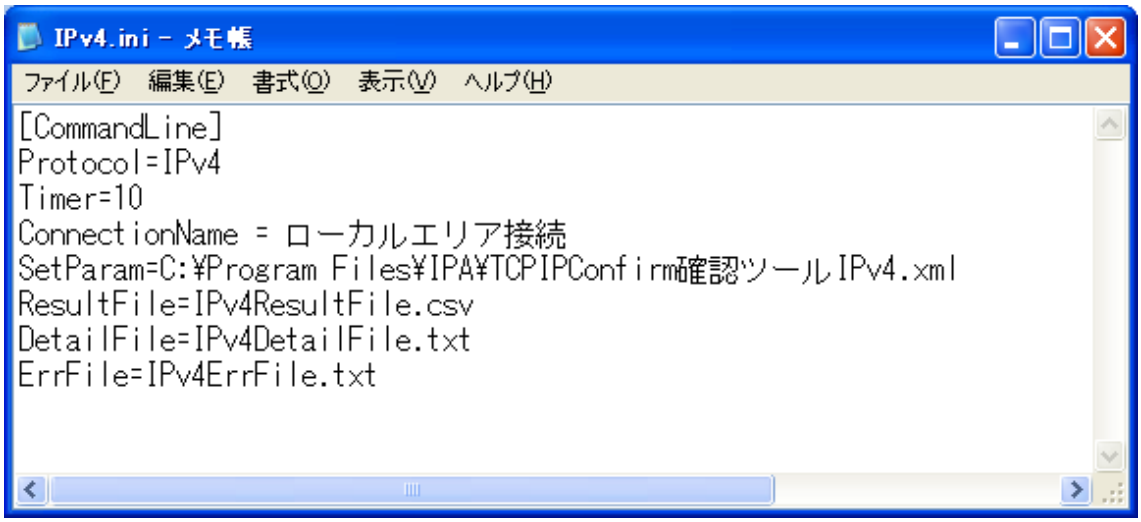
Detailfile	詳細ログの出力ファイルを指定します。指定しなかった時、詳細ログの出力は行われません。	○
ErrFile	エラーログの出力ファイルを指定します。 未指定の時、本ツールのインストールフォルダ¥TCPIP_Err.log”をデフォルトとして使用します	○

- 必須

○ 任意

設定ファイルで使用するファイル名は、絶対パスもしくはファイル名のみにし、相対パスを使用しないでください。また、ファイルの内容は、大文字と小文字が区別されません。

以下に設定ファイルのサンプルを記載します。



5). 項目別確認方法

※項目番号が欠番となっている項目は未実装です。

5)-47.Overlapping Fragment

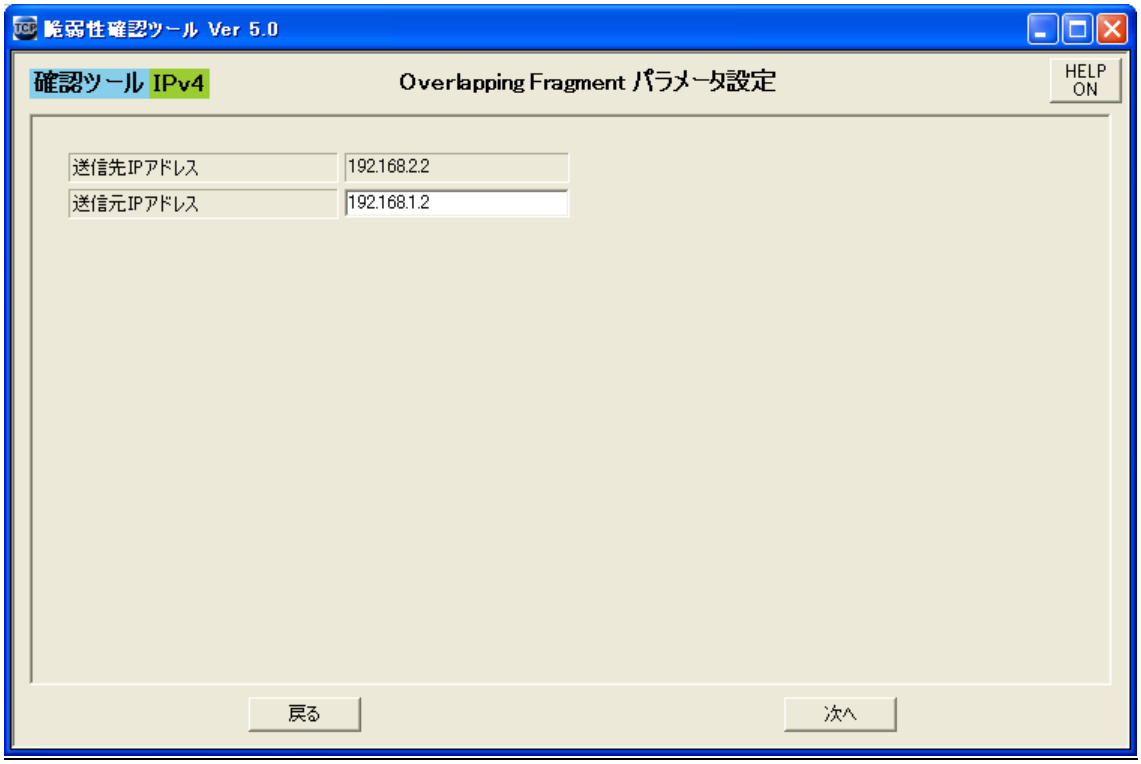
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：5) データを上書きするフラグメントパケットがフィルタリングをすり抜ける問題（Overlapping Fragment Attack）

[IPv4]

ネットワーク構成は TCPIPCheck（脆弱性検証ツール）編 5)-5.Overlapping Fragment を参照してください。

パラメータ設定画面



脆弱性項目パラメータ設定ガイド

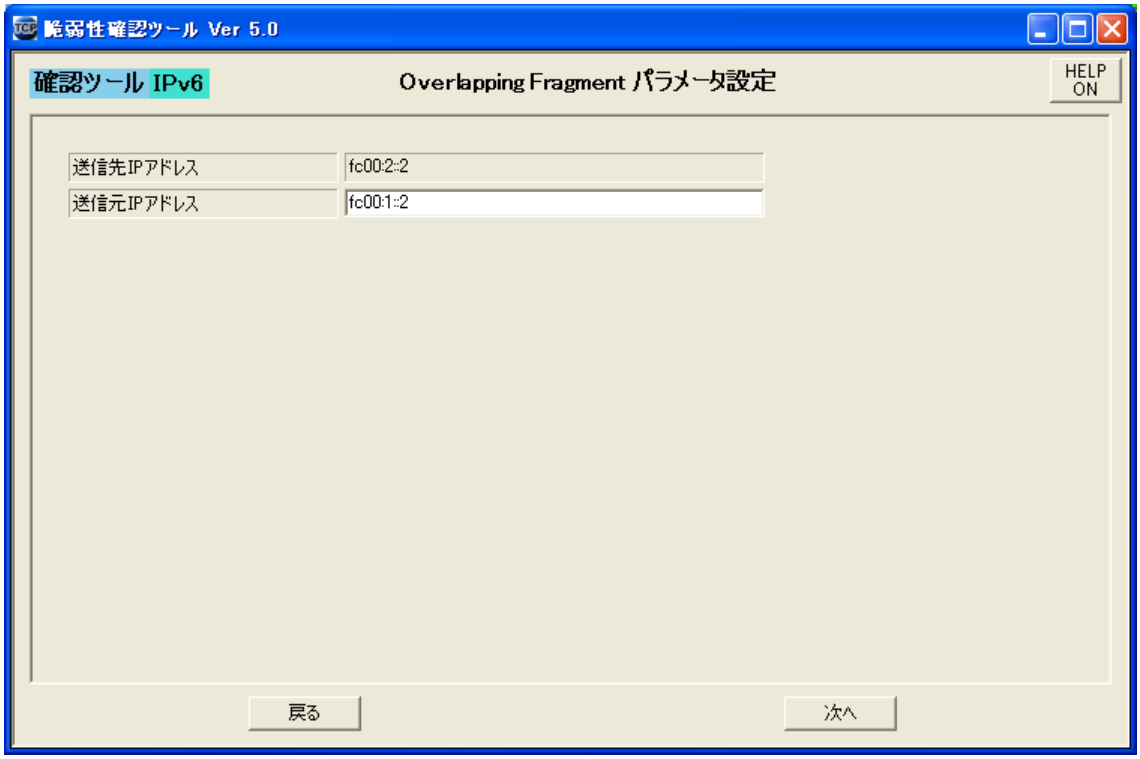
パラメータ名	推奨値
送信元 IP アドレス	TCPIPCheck を実行している機器の IP アドレスを指定してください。但し、TCPIPCheck の Overlapping Fragment パラメータ設定画面で送信元 IP アドレスを指定している時は、この値を指定してください。 空欄にするとパケットを検証する際に送信元 IP アドレスを検

	証対象外にします。より厳密に検証を行う時は、送信元 IP アドレスを指定してください。

[IPv6]

ネットワーク構成は TCPIPCheck（脆弱性検証ツール）編 5)-5.Overlapping Fragment を参照してください。

パラメータ設定画面



脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	TCPIPCheck を実行している機器の IP アドレスを指定してください。但し、TCPIPCheck の Overlapping Fragment パラメータ設定画面で送信元 IP アドレスを指定している時は、この値を指定してください。 空欄にするとパケットを検証する際に送信元 IP アドレスを検証対象外にします。より厳密に検証を行う時は、送信元 IP アドレスを指定してください。

5)-48.Tiny Fragment

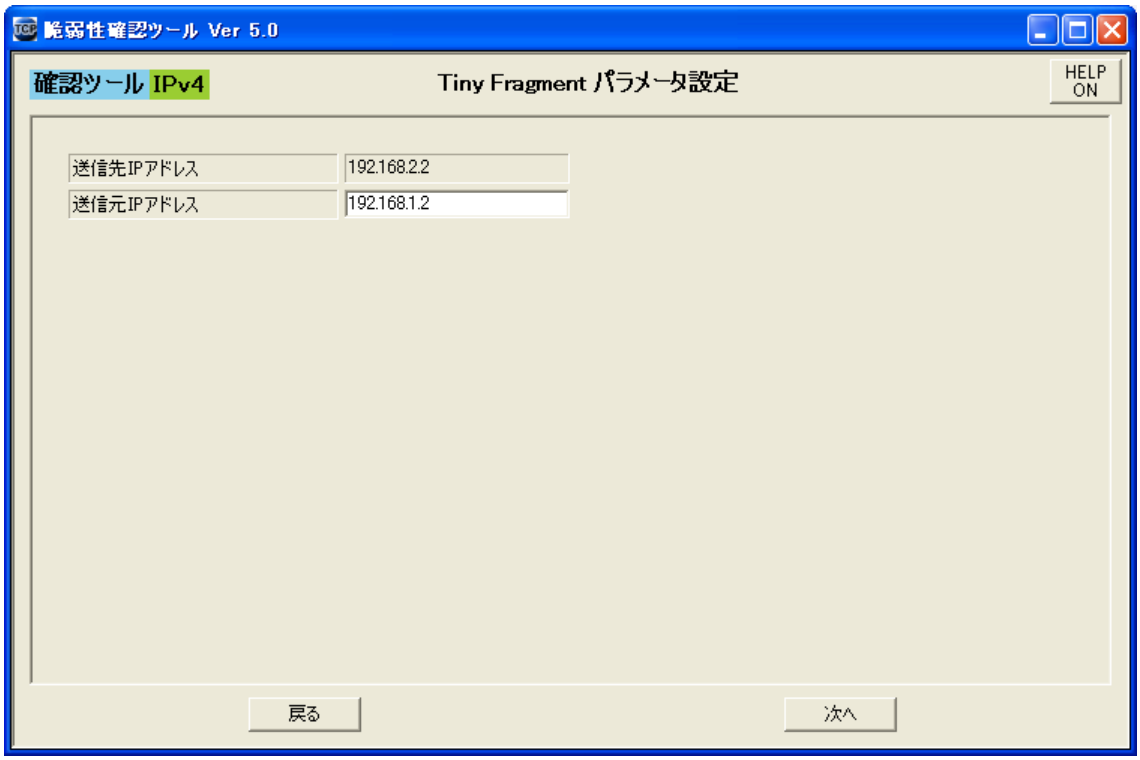
この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：6) 十分に小さい分割パケットがフィルタリングをすり抜ける問題 （Tiny Fragment Attack、Tiny Overlapping Fragment Attack）

[IPv4]

ネットワーク構成は TCPIPCheck（脆弱性検証ツール）編 5)-6.Tiny Fragment を参照してください。

パラメータ設定画面



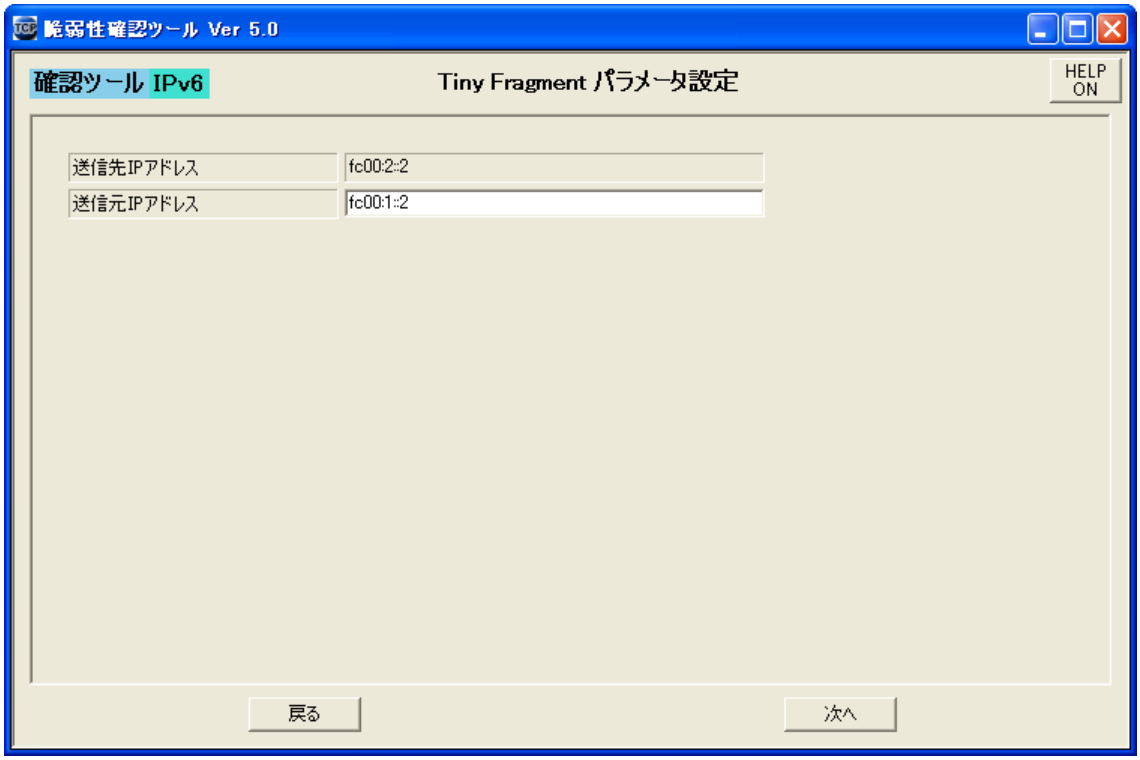
脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	TCPIPCheck を実行している機器の IP アドレスを指定してください。但し、TCPIPCheck の Tiny Fragment パラメータ設定画面で送信元 IP アドレスを指定している時は、この値を指定してください。 空欄にするとパケットを検証する際に送信元 IP アドレスを検証対象外にします。より厳密に検証を行う時は、送信元 IP アドレスを指定してください。

[IPv6]

ネットワーク構成は TCPIPCheck（脆弱性検証ツール）編 5)-6.Tiny Fragment を参照してください。

パラメータ設定画面



脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	TCPIPCheck を実行している機器の IP アドレスを指定してください。但し、TCPIPCheck の Tiny Fragment パラメータ設定画面で送信元 IP アドレスを指定している時は、この値を指定してください。 空欄にするとパケットを検証する際に送信元 IP アドレスを検証対象外にします。より厳密に検証を行う時は、送信元 IP アドレスを指定してください。

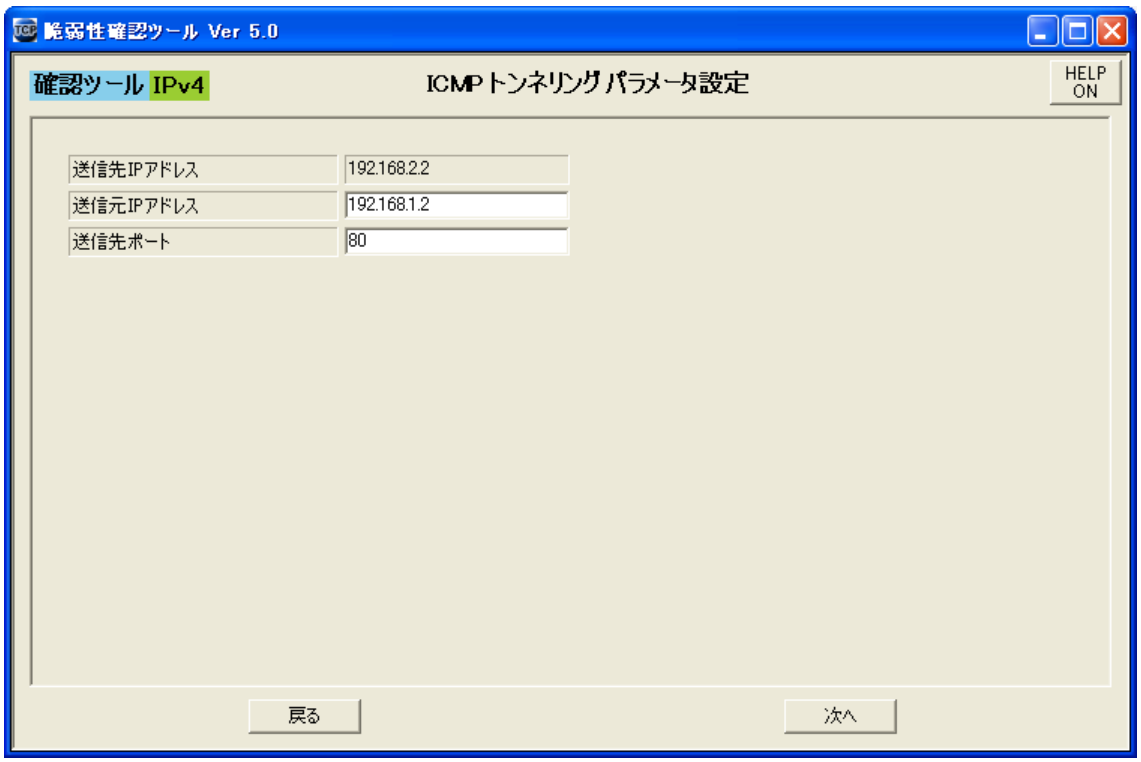
5)-49.ICMP トンネリング

この脆弱性の詳細については、「TCP/IP に係る既知の脆弱性の調査報告書」の以下の項目を参照してください。

参照：15) ICMP ヘッダでカプセル化されたパケットがファイアウォールを通過する問題 [IPv4]

ネットワーク構成は TCPIPCheck（脆弱性検証ツール）編 5)-17.ICMP トンネリングを参照してください。

パラメータ設定画面



脆弱性項目パラメータ設定ガイド

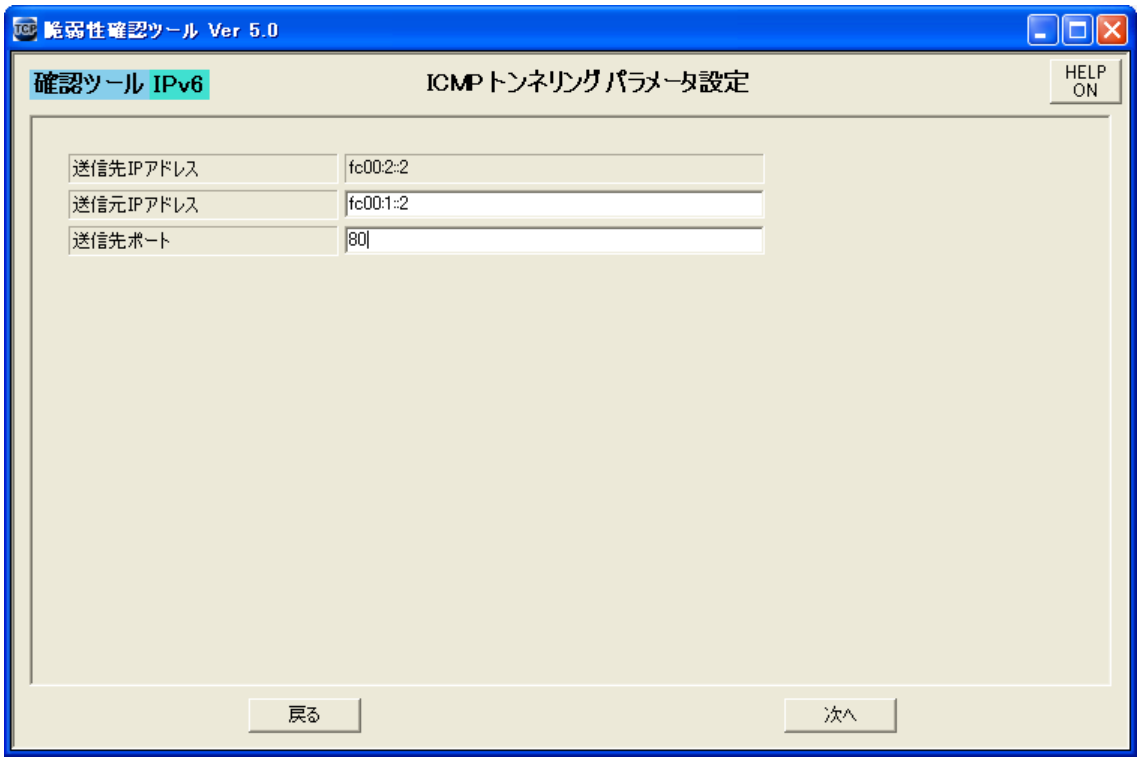
パラメータ名	推奨値
送信元 IP アドレス	TCPIPCheck を実行している機器の IP アドレスを指定してください。但し、TCPIPCheck の ICMP トンネリングパラメータ設定画面で送信元 IP アドレスを指定している時は、この値を指定してください。 空欄にするとパケットを検証する際に送信元 IP アドレスを検証対象外にします。より厳密に検証を行う時は、送信元 IP アドレスを指定してください。
送信先ポート	TCPIPCheck の ICMP トンネリングパラメータ設定画面で指定した送信先ポートを指定してください。 空欄にするとパケットを検証する際に送信先ポートを検証対

	象外にします。より厳密に検証を行う時は、送信先ポートを指定してください。

[IPv6]

ネットワーク構成は TCPIPCheck（脆弱性検証ツール）編 5)-17.ICMP トンネリング**を参照してください。**

パラメータ設定画面



脆弱性項目パラメータ設定ガイド

パラメータ名	推奨値
送信元 IP アドレス	TCPIPCheck を実行している機器の IP アドレスを指定してください。但し、TCPIPCheck の ICMP トンネリングパラメータ設定画面で送信元 IP アドレスを指定している時は、この値を指定してください。 空欄にするとパケットを検証する際に送信元 IP アドレスを検証対象外にします。より厳密に検証を行う時は、送信元 IP アドレスを指定してください。
送信先ポート	TCPIPCheck の ICMP トンネリングパラメータ設定画面で指定した送信先ポートを指定してください。 空欄にするとパケットを検証する際に送信先ポートを検証対象外にします。より厳密に検証を行う時は、送信先ポートを指定してください。